



Sonderheft / Fascicule spécial / Fascicolo speciale / Special issue 44/2003

Bulletin

Bulletin

Sonderheft: Geldwäschereibekämpfung
Fascicule spécial: Lutte contre le blanchiment d'argent
Fascicolo speciale: Lotta contro il riciclaggio di denaro
Special issue: Combating money laundering

44/2003

Eidgenössische Bankenkommission
Commission fédérale des banques
Commissione federale delle banche
Swiss Federal Banking Commission

Bulletin

Sonderheft: Geldwäschereibekämpfung
Fascicule spécial: Lutte contre le blanchiment d'argent
Fascicolo speciale: Lotta contro il riciclaggio di denaro
Special issue: Combating money laundering

44/2003

Eidgenössische Bankenkommision
Commission fédérale des banques
Commissione federale delle banche
Swiss Federal Banking Commission

Herausgeber

Eidg. Bankenkommission
Schwanengasse 12, Postfach, 3001 Bern
Telefon 031 / 322 69 11
Telefax 031 / 322 69 26
E-Mail info@ebk.admin.ch
Internet www.ebk.admin.ch

Editeur

Commission fédérale des banques
Schwanengasse 12, case postale, 3001 Berne
Téléphone 031 / 322 69 11
Téléfax 031 / 322 69 26
E-Mail info@ebk.admin.ch
Internet www.cfb.admin.ch

2

Vertrieb

BBL, Vertrieb Publikationen, CH-3003 Bern
Telefax 031 / 325 50 58
E-Mail verkauf.zivil@bbl.admin.ch
Internet www.bbl.admin.ch/bundespublikationen

Diffusion

OFCL, Diffusion publications, CH-3003 Berne
Téléfax 031 / 325 50 58
E-Mail verkauf.zivil@bbl.admin.ch
Internet www.bbl.admin.ch/bundespublikationen

Bestellnummer

607.144

Numéro de commande

607.144 5.2003 5000 95242

Inhaltsverzeichnis

	Seite
Verzeichnis der Abkürzungen	7
EBK-Geldwäschereiverordnung (d/f/i/e)	15
Bericht zur EBK-Geldwäschereiverordnung (d/f)	95
Vereinbarung über die Standesregeln zur Sorgfaltspflicht der Banken (VSB 03) (d/f/i/e)	230
Basler Ausschuss für Bankenaufsicht: Sorgfaltspflichten der Banken bei der Feststellung der Kundenidentität (d/f/i/e)	353
Anhang: General Guide to Account Opening and Customer Identification (e)	438
Basel Committee on Banking Supervision: Sharing of financial records between jurisdictions in connection with the fight against terrorist financing (e)	448
Financial Action Task Force on Money Laundering: Special Recommendations on Terrorist Financing (e)	454

Sommaire

	Page
Tableau des abréviations	7
Ordonnance de la CFB sur le blanchiment d'argent (a/f/i/e)	15
Rapport sur l'Ordonnance de la CFB sur le blanchiment d'argent (a/f)	95
Convention relative à l'obligation de diligence des banques (CDB 03) (a/f/i/e)	230
Comité de Bâle sur le contrôle bancaire: Devoir de diligence des banques au sujet de la clientèle (a/f/i/e)	353
Annexe: General Guide to Account Opening and Customer Identification (e)	438
Basel Committee on Banking Supervision: Sharing of financial records between jurisdictions in connection with the fight against terrorist financing (e)	448
Financial Action Task Force on Money Laundering: Special Recommendations on Terrorist Financing (e)	454

Sommario

	Pagina
Elenco delle abbreviazioni	7
Ordinanza CFB sul riciclaggio di denaro (t/f/i/e)	15
Rapporto sull'ordinanza CFB sul riciclaggio di denaro (t/f)	95
Convenzione relativa all'obbligo di diligenza delle banche (CDB 03) (t/f/i/e)	230
Comitato di Basilea per la vigilanza bancaria: Dovere di diligenza delle banche nell'identificazione della clientela (t/f/i/e)	353
Allegato: General Guide to Account Opening and Customer Identification (e)	438
Basel Committee on Banking Supervision: Sharing of financial records between jurisdictions in connection with the fight against terrorist financing (e)	448
Financial Action Task Force on Money Laundering: Special Recommendations on Terrorist Financing (e)	454

Table of contents

	Side
List of abbreviations	7
SFBC Money Laundering Ordinance (g/f/i/e)	15
Report on the SFBC Money Laundering Ordinance (g/f)	95
Agreement on the Swiss banks' code of conduct with regard to the exercise of due diligence (CDB 03) (g/f/i/e)	230
Basel Committee on Banking Supervision: Customer due diligence for banks (g/f/i/e)	353
Attachment: General Guide to Account Opening and Customer Identification (e)	438
Basel Committee on Banking Supervision: Sharing of financial records between jurisdictions in connection with the fight against terrorist financing (e)	448
Financial Action Task Force on Money Laundering: Special Recommendations on Terrorist Financing (e)	454

Verzeichnis der Abkürzungen
Tableau des abréviations
Elenco delle abbreviazioni
English abbreviations

ABV	Verordnung über die ausländischen Banken in der Schweiz vom 21. Oktober 1996 (Auslandbankenverordnung, SR 952.111) OBE/OBE/FBO
AFG	Bundesgesetz über die Anlagefonds vom 18. März 1994 (Anlagefondsgesetz, SR 951.31) LFP/LFI/IFA
AFV	Verordnung über die Anlagefonds vom 19. Oktober 1994 (SR 951.311) OFP/OFI/IFO
AFV-EBK	Verordnung der Eidgenössischen Bankenkommision über die Anlagefonds vom 27. Oktober 1994 (SR 951.311.1) OFP-CFB/OFI-CFB/IFO-SFBC
APA	Federal Act on Administrative Procedure of 20 December 1968 (Administrative Procedure Act 1968) VwVG/PA/PA
AS	Amtliche Sammlung des Bundesrechts RO/RU/RO
ATF	Arrêts du Tribunal fédéral suisse BGE/DTF/ATF
ATF	Decisions of the Federal Supreme Court BGE/ATF/DTF
BA	Federal Banking Act of 8 November 1934 (Banking Act 1934) BankG/LB/LBCR
BankG	Bundesgesetz über die Banken und Sparkassen vom 8. November 1934 (Bankengesetz, SR 952.0) LB/LBCR/BA
BankV	Verordnung über die Banken und Sparkassen vom 17. Mai 1972 (Bankenverordnung, SR 952.02) OB/OBCR/BO
BBl	Bundesblatt FF/FF/FF

BEHG	Bundesgesetz über die Börsen und den Effektenhandel vom 24. März 1995 (Börsengesetz, SR 954.1) LBVM/LBVM/SESTA
BEHV	Verordnung über die Börsen und den Effektenhandel vom 2. Dezember 1996 (Börsenverordnung, SR 954.11) OBVM/OBVM/SESTO
BEHV-EBK	Verordnung der Eidgenössischen Bankenkommision über die Börsen und den Effektenhandel vom 25. Juni 1997 (Börsenverordnung-EBK, SR 954.193) OBVM-CFB/OBVM-CFB/SESTO-SFBC
BGE	Entscheidungen des Schweizerischen Bundesgerichts ATF/DTF/ATF
BO	Ordinance to the Federal Banking Act of 17 May 1972 (Banking Ordinance 1972) BankV/OB/OBCR
BPG	Bundespersongesetz vom 24. März 2000 (SR 172.220.1) LPers/LPers
BStP	Bundesgesetz über die Bundesstrafrechtspflege vom 15. Juni 1934 (SR 312.0) PPF/PP
BZP	Bundesgesetz über den Bundeszivilprozess vom 4. Dezember 1947 (SR 273) PCF/PC
CDB	Convention relative à l'obligation de diligence des banques VSB/CDB
CDB	Convenzione relativa all'obbligo di diligenza delle banche VSB/CDB
CFB	Commission fédérale des banques EBK/CFB/SFBC
CFB	Commissione federale delle banche EBK/CFB/SFBC
CP	Code pénal suisse du 21 décembre 1937 (RS 311.0) StGB/CP

CP	Codice penale svizzero del 21 dicembre 1937 (SR 311.0) StGB/CP
DTF	Decisioni del Tribunale federale svizzero BGE/ATF/ATF
EBK	Eidgenössische Bankenkommision CFB/CFB/SFBC
EBK-GebV	Verordnung über die Erhebung von Abgaben und Gebühren durch die Eidg. Bankenkommision vom 2. Dezember 1996 (SR 611.014) Oém-CFB/Oem-CFB
FBO	Ordinance on Foreign Banks in Switzerland of 21 October 1996 (Foreign Banks Ordinance 1996) ABV/OBE/OBE
FF	Federal journal BBI/FF/FF
FF	Feuille fédérale BBI/FF/FF
FF	Foglio federale BBI/FF/FF
GwG	Bundesgesetz zur Bekämpfung der Geldwäscherei (SR 955.0) LBAL/LRD
GwV EBK	Verordnung der Eidgenössischen Bankenkommision zur Verhin- derung von Geldwäscherei vom 18. Dezember 2002 (SR 955.022) OBA-CFB/ORD-CFB/MLO SFBC
IFA	Federal Act on Investment Funds of 18 March 1994 (Investment Fund Act 1994) AFG/LFP/LFI
IFO	Ordinance of the Federal Council on Investment Funds of 19 October 1994 (Investment Fund Ordinance 1994) AFV/OFP/OFI
IFO-SFBC	Ordinance of the Swiss Federal Banking Commission on Invest- ment Funds of 27 October 1994 (Investment Fund Ordinance of the Banking Commission 1994) AFV-EBK/OFP-CFB/OFI-CFB

LB	Loi fédérale sur les banques et les caisses d'épargne du 8 novembre 1934 (Loi sur les banques, RS 952.0) BankG/LBCR/BA
LBA	Loi sur le blanchiment d'argent (RS 955.0) GwG/LRD
LBCR	Legge federale su le banche e le casse di risparmio dell'8 novembre 1934 (Legge sulle banche, RS 952.0) BankG/LB/BA
LBVM	Legge federale sulle borse e il commercio di valori mobiliari del 24 marzo 1995 (Legge sulle borse, RS 954.1) BEHG/LBVM/SESTA
LBVM	Loi fédérale sur les bourses et le commerce des valeurs mobilières du 24 mars 1995 (Loi sur les bourses, RS 954.1) BEHG/LBVM/SESTA
LFI	Legge federale sui fondi d'investimento del 18 marzo 1994 (RS 951.31) AFG/LFP/IFA
LFP	Loi fédérale sur les fonds de placement du 18 mars 1994 (RS 951.31) AFG/LFI/IFA
LPers	Loi sur le personnel de la Confédération du 24 mars 2000 (RS 172.220.1) BPG/LPers
LPers	Legge sul personale federale del 24 marzo 2000 (SR 172.220.1) BPG/LPers
LRD	Legge sur riciclaggio di denaro (RS 955.0) GwG/LBA
MLO SFBC	Ordinance of the Swiss Federal Banking Commission Concerning the Prevention of Money Laundering of 18 December 2002 GwV EBK/OBA-CFB/ORD-CFB
OB	Ordonnance sur les banques et les caisses d'épargne du 17 mai 1972 (Ordonnance sur les banques, RS 952.02) BankV/OBCR/BO

OBA-CFB	Ordonnance de la CFB sur le blanchiment d'argent du 18 décembre 2002 (RS 955.022) GwV EBK/ORD-CFB/MLO SFBC
OBCR	Ordinanza su le banche e le casse di risparmio del 17 maggio 1972 (Ordinanza sulle banche, RS 952.02) BankV/OB/BO
OBE	Ordinanza concernente le banche estere in Svizzera del 21 ottobre 1996 (Ordinanza sulle banche estere, RS 952.111) ABV/OBE/FBO
OBE	Ordonnance concernant les banques étrangères en Suisse du 21 octobre 1996 (Ordonnance sur les banques étrangères, RS 952.111) ABV/OBE/FBO
OBVM	Ordinanza sulle borse e il commercio di valori mobiliari del 2 dicembre 1996 (Ordinanza sulle borse, RS 954.11) BEHV/OBVM/SESTO
OBVM	Ordonnance sur les bourses et le commerce des valeurs mobilières du 2 décembre 1996 (Ordonnance sur les bourses, RS 954.11) BEHV/OBVM/SESTO
OBVM-CFB	Ordinanza della Commissione federale delle banche sulle borse e il commercio di valori mobiliari del 25 giugno 1997 (Ordinanza sulle borse della CFB, RS 954.193) BEHV-EBK/OBVM-CFB/SESTO-SFBC
OBVM-CFB	Ordonnance de la Commission fédérale des banques sur les bourses et le commerce des valeurs mobilières du 25 juin 1997 (Ordonnance sur les bourses de la CFB, RS 954.193) BEHV-EBK/OBVM-CFB/SESTO-SFBC
Oem-CFB	Ordinanza sulla riscossione di tasse e emolumenti da parte della Commissione federale delle banche del 2 dicembre 1996 (RS 611.014) EBK-GebV/Oém-CFB

Oém-CFB	Ordonnance réglant la perception de taxes et d'émoluments par la Commission fédérale des banques du 2 décembre 1996 (RS 611.014) EBK-GebV/Oem-CFB
OFI	Ordinanza sui fondi d'investimento del 19 ottobre 1994 (RS 951.311) AFV/OFP/IFO
OFI-CFB	Ordinanza della Commissione federale delle banche sui fondi d'investimento del 27 ottobre 1994 (RS 951.311.1) AFV-EBK/OFP-CFB/IFO-SFBC
OFP	Ordonnance sur les fonds de placement du 19 octobre 1994 (RS 951.311) AFV/OFI/IFO
OFP-CFB	Ordonnance de la Commission fédérale des banques sur les fonds de placement du 27 octobre 1994 (RS 951.311.1) AFV-EBK/OFI-CFB/IFO-SFBC
OG	Bundesgesetz über die Organisation der Bundesrechtspflege vom 16. Dezember 1943 (Bundesrechtspflegegesetz, SR 173.110) OJ/OG
OG	Legge federale sull'organizzazione giudiziaria del 16 dicembre 1943 (Organizzazione giudiziaria, RS 173.110) OG/OJ
OJ	Loi fédérale d'organisation judiciaire du 16 décembre 1943 (Organisation judiciaire, RS 173.110) OG/OG
ORD-CFB	Ordinanza CFB sul riciclaggio di denaro del 18 dicembre 2002 (RS 955.022) GwV EBK/OBA-CFB/MLO SFBC
PA	Legge federale sulla procedura amministrativa del 20 dicembre 1968 (RS 172.021) VwVG/PA/APA

PA	Loi fédérale sur la procédure administrative du 20 décembre 1968 (RS 172.021) VwVG/PA/APA
PC	Legge di procedura civile federale del 4 dicembre 1947 (RS 273) BZP/PCF
PCF	Loi fédérale de procédure civile fédérale du 4 décembre 1947 (RS 273) BZP/PC
PP	Legge federale sulla procedura penale del 15 giugno 1934 (RS 312.0) BStP/PPF
PPF	Loi fédérale sur la procédure pénale du 15 juin 1934 (RS 312.0) BStP/PP
R-CFB	Regolamento della Commissione federale delle banche del 20 no- vembre 1997 (RS 952.721) R-EBK/R-CFB
R-CFB	Règlement de la Commission fédérale des banques du 20 novem- bre 1997 (RS 952.721) R-EBK/R-CFB
R-EBK	Reglement über die Eidgenössische Bankenkommision vom 20. November 1997 (SR 952.721) R-CFB/R-CFB
RO	Official chronological collection of the federal legislation AS/RO/RU
RO	Recueil officiel des lois fédérales AS/RU/RO
RS	Raccolta sistematica del diritto federale SR/RS/RS
RS	Recueil systématique du droit fédéral SR/RS/RS
RS	Systematic collection of the federal legislation SR/RS/RS

RU	Raccolta ufficiale delle leggi federali AS/RO/RO
SESTA	Federal Act on Securities Exchanges and Securities Trading of 24 March 1995 (Securities Act 1995) BEHG/LBVM/LBVM
SESTO	Ordinance of the Federal Council to the Federal Act on Securities Exchanges and Securities Trading of 2 December 1996 (Securities Ordinance 1996) BEHV/OBVM/OBVM
SESTO-SFBC	Ordinance of the Swiss Federal Banking Commission to the Fed- eral Act on Securities Exchanges and Securities Trading of 25 June 1997 (Securities Ordinance of the Banking Commission 1997) BEHV-EBK/OBVM-CFB/OBVM-CFB
SFBC	Swiss Federal Banking Commission EBK/CFB/CFB
SR	Systematische Sammlung des Bundesrechts RS/RS/RS
StGB	Schweizerisches Strafgesetzbuch vom 21. Dezember 1937 (SR 311.0) CP/CP
VG	Bundesgesetz über die Verantwortlichkeit des Bundes sowie seiner Behördenmitglieder und Beamten vom 14. März 1958 (Verant- wortlichkeitsgesetz, SR 170.32)
VSB	Vereinbarung über die Standesregeln zur Sorgfaltspflicht der Banken CDB/CDB
VStrR	Bundesgesetz über das Verwaltungsstrafrecht vom 22. März 1974 (SR 313.0)
VwOG	Bundesgesetz über die Organisation und die Geschäftsführung des Bundesrates und der Bundesverwaltung vom 19. September 1978 (SR 172.010)
VwVG	Bundesgesetz über das Verwaltungsverfahren vom 20. Dezember 1968 (SR 172.021) PA/PA/APA

Verordnung der Eidgenössischen Bankenkommission zur Verhinderung von Geldwäscherei (EBK-Geldwäschereiverordnung, GwV EBK)

vom 18. Dezember 2002

*Die Eidgenössische Bankenkommission,
gestützt auf die Artikel 16 Absatz 1 und 41 des Geldwäschereigesetzes
vom 10. Oktober 1997¹,
verordnet:*

1. Abschnitt: Allgemeine Bestimmungen

Art. 1 Begriffe

In dieser Verordnung gelten als:

- a. politisch exponierte Personen:
 1. folgende Personen mit prominenten öffentlichen Funktionen im Ausland: Staats- und Regierungschefs, hohe Politikerinnen und Politiker auf nationaler Ebene, hohe Funktionäre in Verwaltung, Justiz, Militär und Parteien auf nationaler Ebene, die obersten Organe staatlicher Unternehmen von nationaler Bedeutung,
 2. Unternehmen und Personen, welche den genannten Personen aus familiären, persönlichen oder geschäftlichen Gründen erkennbar nahe stehen;
- b. professionelle Notenhändler: In- oder ausländische Nichtbanken (Unternehmen oder Personen), die Noten kaufen und verkaufen und damit einen wesentlichen Umsatz oder Ertrag erzielen;
- c. terroristische Organisationen: Kriminelle Organisationen im Sinne von Artikel 260^{ter} des Strafgesetzbuches²;
- d. Gruppengesellschaften: Gesellschaften, die ein Finanzintermediär nach Artikel 2 Absatz 1 nach den Eigenmittelvorschriften zu konsolidieren hat.

SR 955.022

¹ SR 955.0

² SR 311.0

Art. 2 Geltungsbereich

¹ Diese Verordnung gilt für Finanzintermediäre nach Artikel 2 Absatz 2 Buchstaben a, b und d des Geldwäschereigesetzes, ausser für Fondsleitungen, wenn die in dieser Verordnung und im Geldwäschereigesetz enthaltenen Pflichten von der Depotbank übernommen werden.

² Die Bankenkommission kann eine inländische Gruppengesellschaft eines Finanzintermediärs nach Absatz 1 auf ihr Gesuch hin hinsichtlich der Einhaltung der Pflichten dieser Verordnung beaufsichtigen, sofern:

- a. sie eine Finanztätigkeit nach Artikel 2 Absatz 3 des Geldwäschereigesetzes ausübt;
- b. sie die Voraussetzungen von Artikel 14 Absatz 2 des Geldwäschereigesetzes erfüllt;
- c. sie anerkennt, dass die Bankenkommission ihr gegenüber Massnahmen nach den Artikeln 19 und 20 des Geldwäschereigesetzes treffen kann;
- d. die Gruppe zusichert, die Einhaltung dieser Verordnung zu überwachen und durchzusetzen;
- e. die Gruppe zusichert, ihre externe Revisionsstelle zu beauftragen, die Einhaltung dieser Verordnung zu prüfen und dazu im Revisionsbericht über die Gruppe für jede erfasste Gruppengesellschaft einzeln Stellung zu nehmen.

³ Die Bankenkommission veröffentlicht eine Liste der von ihr nach Absatz 2 überwachten Gruppengesellschaften.

Art. 3 Zweigniederlassungen und Gruppengesellschaften im Ausland

¹ Der Finanzintermediär sorgt dafür, dass seine Zweigniederlassungen oder im Finanzbereich tätige Gruppengesellschaften im Ausland die grundlegenden Prinzipien dieser Verordnung befolgen.

² Er informiert die Bankenkommission, wenn:

- a. lokale Vorschriften der Befolgung der grundlegenden Prinzipien dieser Verordnung entgegenstehen; oder
- b. ihm daraus ein ernsthafter Wettbewerbsnachteil entsteht.

³ Die Meldung verdächtiger Transaktionen oder Geschäftsbeziehungen und allenfalls eine Vermögenssperre richten sich nach den Vorschriften des Gastlandes.

2. Abschnitt: Grundsätze

Art. 4 Verbot der Annahme von Vermögenswerten aus Korruption und anderen Verbrechen

¹ Der Finanzintermediär darf keine Vermögenswerte entgegennehmen, von denen er weiss oder annehmen muss, dass sie aus einem Verbrechen herrühren, auch wenn es im Ausland begangen wurde.

² Aus einem Verbrechen herrührende Vermögenswerte sind insbesondere auch solche, welche aus Bestechung, Veruntreuung öffentlicher Vermögenswerte, Amtsmissbrauch oder ungetreuer Amtsführung stammen.

³ Die fahrlässige Annahme aus einem Verbrechen herrührender Vermögenswerte kann die vom Finanzintermediär geforderte Gewähr für eine einwandfreie Geschäftstätigkeit in Frage stellen.

Art. 5 Verbot von Geschäftsbeziehungen mit kriminellen und terroristischen Organisationen

Der Finanzintermediär darf keine Geschäftsbeziehungen mit Unternehmen und Personen unterhalten, von denen er weiss oder annehmen muss, dass sie eine terroristische oder eine andere kriminelle Organisation bilden oder einer solchen Organisation angehören, sie unterstützen oder finanzieren.

Art. 6 Korrespondenzbankbeziehungen

¹ Die Bestimmungen dieser Verordnung gelten auch für Korrespondenzbankbeziehungen.

² Der Finanzintermediär darf keine Geschäftsbeziehungen mit Banken führen, welche am Inkorporationsort keine physische Präsenz unterhalten, sofern sie nicht Teil einer angemessen konsolidiert überwachten Finanzgruppe sind.

3. Abschnitt: Organisatorische Massnahmen

Art. 7 Geschäftsbeziehungen mit erhöhten Risiken

¹ Der Finanzintermediär entwickelt Kriterien, welche auf Geschäftsbeziehungen mit erhöhten Rechts- und Reputationsrisiken hinweisen.

² Als Kriterien kommen je nach Geschäftsaktivitäten des Finanzintermediärs insbesondere in Frage:

- a. Sitz oder Wohnsitz der Vertragspartei und des wirtschaftlich Berechtigten oder deren Staatsangehörigkeit;
- b. Art und Ort der Geschäftstätigkeit der Vertragspartei und des wirtschaftlich Berechtigten;
- c. Fehlen eines persönlichen Kontakts zur Vertragspartei sowie zum wirtschaftlich Berechtigten;
- d. Art der verlangten Dienstleistungen oder Produkte;
- e. Höhe der eingebrachten Vermögenswerte;
- f. Höhe der Zu- und Abflüsse von Vermögenswerten;
- g. Herkunfts- oder Zielland häufiger Zahlungen.

³ Als Geschäftsbeziehungen mit erhöhten Risiken gelten in jedem Fall diejenigen mit politisch exponierten Personen.

⁴ Der Finanzintermediär ermittelt und kennzeichnet intern die Geschäftsbeziehungen mit erhöhten Risiken nach den Absätzen 2 und 3.

Art. 8 Transaktionen mit erhöhten Risiken

¹ Der Finanzintermediär entwickelt Kriterien zur Erkennung von Transaktionen mit erhöhten Rechts- und Reputationsrisiken.

² Als Kriterien kommen je nach Geschäftsaktivitäten des Finanzintermediärs insbesondere in Frage:

- a. die Höhe der Zu- und Abflüsse von Vermögenswerten;
- b. erhebliche Abweichungen gegenüber den in der Geschäftsbeziehung üblichen Transaktionsarten, -volumina und -frequenzen;
- c. erhebliche Abweichungen gegenüber den in vergleichbaren Geschäftsbeziehungen üblichen Transaktionsarten, -volumina und -frequenzen.

³ Als Transaktionen mit erhöhten Risiken gelten in jedem Fall Transaktionen:

- a. bei denen am Anfang der Geschäftsbeziehung auf ein Mal oder gestaffelt Vermögenswerte im Gegenwert von mehr als 100 000 Franken physisch eingebracht werden;
- b. welche Anhaltspunkte auf Geldwäscherei (Anhang) aufweisen.

Art. 9 Globale Überwachung der Rechts- und Reputationsrisiken

¹ Der Finanzintermediär, welcher Zweigniederlassungen im Ausland besitzt oder eine Finanzgruppe mit ausländischen Gesellschaften leitet, muss seine mit Geldwäscherei und Terrorismusfinanzierung verbundenen Rechts- und Reputationsrisiken global erfassen, begrenzen und überwachen.

² Er hat sicherzustellen, dass:

- a. die internen Überwachungsorgane und die externe Revisionsstelle der Gruppe im Bedarfsfall einen Zugang zu Informationen über einzelne Geschäftsbeziehungen in allen Gruppengesellschaften haben. Nicht erforderlich ist eine zentrale Datenbank der Vertragsparteien und der wirtschaftlich Berechtigten auf Gruppenebene oder ein zentraler Zugang der internen Überwachungsorgane der Gruppe zu lokalen Datenbanken;
- b. die Gruppengesellschaften den zuständigen Organen der Gruppe die für die globale Überwachung der Rechts- und Reputationsrisiken wesentlichen Informationen zur Verfügung stellen.

³ Stellt ein Finanzintermediär fest, dass der Zugang zu Informationen über Vertragsparteien und wirtschaftlich Berechtigte in bestimmten Ländern aus rechtlichen oder praktischen Gründen ausgeschlossen oder ernsthaft behindert ist, so informiert er die Bankenkommission unverzüglich darüber.

⁴ Der Finanzintermediär, welcher Teil einer in- oder ausländischen Finanzgruppe bildet, gewährt den internen Überwachungsorganen und der externen Revisionsstelle der Gruppe im Bedarfsfall Zugang zu Informationen über bestimmte Geschäftsbeziehungen, soweit dies zur

globalen Überwachung von Rechts- und Reputationsrisiken notwendig ist.

Art. 10 Interne Weisungen zur Bekämpfung der Geldwäscherei

¹ Der Finanzintermediär erlässt interne Weisungen zur Bekämpfung der Geldwäscherei und gibt sie den Kundenbetreuerinnen und Kundenbetreuern und allen anderen betroffenen Mitarbeiterinnen und Mitarbeitern bekannt.

² Er regelt darin insbesondere:

- a. welche Kriterien er zur Ermittlung von Geschäftsbeziehungen mit erhöhten Risiken nach Artikel 7 anwendet;
- b. welche Kriterien er zur Erkennung von Transaktionen mit erhöhten Risiken nach Artikel 8 Absatz 1 und 2 anwendet;
- c. wie er diese erhöhten Risiken erfasst, begrenzt und überwacht;
- d. die Grundzüge der Transaktionsüberwachung nach Artikel 12;
- e. die Fälle, in denen die interne Geldwäschereifachstelle beigezogen und das oberste Geschäftsführungsorgan informiert werden müssen;
- f. die Grundzüge der Ausbildung der Mitarbeiterinnen und Mitarbeiter;
- g. die Geschäftspolitik hinsichtlich politisch exponierter Personen;
- h. die Zuständigkeit für Meldungen an die Meldestelle für Geldwäscherei;
- i. die Betragsgrenzen nach Artikel 7 Absatz 2 Buchstaben e und f und Artikel 8 Absatz 2 Buchstabe a.

³ Die Weisungen sind durch den Verwaltungsrat oder das oberste Geschäftsführungsorgan zu erlassen.

Art. 11 Ausbildung des Personals

Der Finanzintermediär sorgt für die regelmässige Ausbildung der Kundenbetreuerinnen und Kundenbetreuer und aller anderen betroffenen Mitarbeiterinnen und Mitarbeiter hinsichtlich der für sie wesentlichen Aspekte der Geldwäschereibekämpfung.

Art. 12 Systeme zur Transaktionsüberwachung

¹ Der Finanzintermediär sorgt für eine wirksame Transaktionsüberwachung und betreibt ein informatikgestütztes System, das hilft, Transaktionen mit erhöhten Risiken nach Artikel 8 Absätze 1, 2 und 3 Buchstabe a zu ermitteln.

² Die durch das Überwachungssystem ermittelten Transaktionen sind innert angemessener Frist auszuwerten. Wenn nötig, sind zusätzliche Abklärungen nach Artikel 17 durchzuführen.

³ Finanzintermediäre mit einer geringen Anzahl Vertragsparteien und wirtschaftlich Berechtigten oder Transaktionen können auf ein informatikgestütztes Überwachungssystem verzichten, wenn sie ihre externe Revisionsstelle beauftragen, ihre Transaktionsüberwachung jährlich einer Schwerpunktsprüfung zu unterziehen.

Art. 13 Interne Geldwäschereifachstelle

¹ Der Finanzintermediär hat eine oder mehrere qualifizierte Personen als Geldwäschereifachstelle zu bezeichnen. Diese unterstützt und berät die Linienverantwortlichen und die Geschäftsleitung bei der Umsetzung dieser Verordnung, ohne ihnen die Verantwortung dafür abzunehmen.

² Die Geldwäschereifachstelle:

- a. bereitet die internen Weisungen zur Bekämpfung der Geldwäscherei vor;
- b. überwacht in Absprache mit der internen und externen Revision und den Linienverantwortlichen den Vollzug der internen Weisungen zur Bekämpfung der Geldwäscherei;
- c. plant und überwacht die interne Ausbildung zur Bekämpfung der Geldwäscherei;
- d. legt die Parameter für das System zur Transaktionsüberwachung nach Artikel 12 fest;
- e. veranlasst die Auswertung der durch das Transaktionsüberwachungssystem erzeugten Meldungen;
- f. veranlasst zusätzliche Abklärungen nach Artikel 17 oder führt sie selbst durch;

g. stellt sicher, dass das verantwortliche Geschäftsführungsorgan die für seinen Entscheid über die Aufnahme oder Weiterführung von Geschäftsbeziehungen nach Artikel 22 Absatz 1 nötigen Entscheidungsgrundlagen erhält.

³ Der Finanzintermediär kann unter seiner Verantwortung auch fachkundige externe Personen als Geldwäschereifachstelle bezeichnen, wenn:

- a. er von seiner Grösse oder Organisation her nicht in der Lage ist, eine eigene Fachstelle einzurichten; oder
- b. die Einrichtung einer solchen unzweckmässig wäre.

4. Abschnitt: Allgemeine Sorgfaltspflichten

Art. 14 Identifizierung der Vertragspartei und Feststellung des wirtschaftlich Berechtigten

¹ Für die Identifizierung der Vertragsparteien und die Feststellung der wirtschaftlich Berechtigten gelten für alle Finanzintermediäre die Bestimmungen der von den Banken mit der Schweizerischen Bankiervereinigung abgeschlossenen «Vereinbarung über die Standesregeln zur Sorgfaltspflicht der Banken» vom 2. Dezember 2002 (VSB 2003).

² Die Verletzung der VSB 2003 kann die vom Finanzintermediär geforderte Gewähr für eine einwandfreie Geschäftstätigkeit in Frage stellen.

Art. 15 Angabe der Auftraggeber bei Zahlungsaufträgen

¹ Der Finanzintermediär gibt bei allen Zahlungsaufträgen ins Ausland den Namen, die Kontonummer und das Domizil der auftraggebenden Vertragspartei oder den Namen und eine Identifizierungsnummer an.

² Der Finanzintermediär kann aus berechtigten Gründen, wie bei Daueraufträgen, von diesen Angaben absehen. Er klärt diese Gründe ab und dokumentiert sie.

Art. 16 Professioneller Notenhandel

¹ Professioneller Notenhandel ist nur zulässig mit Notenhändlern,

welche die Kriterien für eine vertrauenswürdige Korrespondenzbankbeziehung erfüllen.

² Vor Aufnahme der Geschäftsbeziehung hat der Finanzintermediär sich über die Geschäftstätigkeit des Notenhändlers zu erkundigen und Handelsauskünfte sowie Referenzen einzuholen.

³ Der Finanzintermediär legt Umsatz- und Kreditlimiten für seinen professionellen Notenhandel insgesamt und für jede Gegenpartei fest, überprüft diese mindestens einmal jährlich und überwacht ihre Einhaltung dauernd.

⁴ Der Finanzintermediär, der den professionellen Notenhandel betreibt, erlässt dazu Weisungen, welche grundsätzlich vom obersten Geschäftsführungsorgan zu beschliessen sind.

5. Abschnitt: Erhöhte Sorgfaltspflichten

Art. 17 Zusätzliche Abklärungen bei erhöhten Risiken

¹ Bei Geschäftsbeziehungen oder Transaktionen mit erhöhten Risiken trifft der Finanzintermediär mit angemessenem Aufwand zusätzliche Abklärungen.

² Abzuklären ist je nach den Umständen namentlich:

- a. ob die Vertragspartei an den eingebrachten Vermögenswerten wirtschaftlich berechtigt ist;
- b. die Herkunft der eingebrachten Vermögenswerte;
- c. der Verwendungszweck abgezogener Vermögenswerte;
- d. die Plausibilität grösserer Zahlungseingänge;
- e. der Ursprung des Vermögens der Vertragspartei und des wirtschaftlich Berechtigten;
- f. die berufliche oder geschäftliche Tätigkeit der Vertragspartei und des wirtschaftlich Berechtigten;
- g. ob es sich bei der Vertragspartei oder dem wirtschaftlich Berechtigten um eine politisch exponierte Person handelt;
- h. bei juristischen Personen: wer diese beherrscht.

Art. 18 Abklärungsmittel

¹ Die Abklärungen umfassen je nach den Umständen namentlich:

- a. das Einholen schriftlicher oder mündlicher Auskünfte der Vertragsparteien oder wirtschaftlich Berechtigten;
- b. Besuche am Ort der Geschäftstätigkeit der Vertragsparteien und wirtschaftlich Berechtigten;
- c. eine Konsultation allgemein zugänglicher öffentlicher Quellen und Datenbanken;
- d. allenfalls Erkundigungen bei vertrauenswürdigen Personen.

² Die Abklärungen wahren die Privatsphäre der Betroffenen.

³ Der Finanzintermediär überprüft die Ergebnisse der Abklärungen auf ihre Plausibilität hin und dokumentiert sie.

Art. 19 Delegation der zusätzlichen Abklärungen an Dritte

¹ Der Finanzintermediär darf Personen und Unternehmen mit den zusätzlichen Abklärungen in einer schriftlichen Vereinbarung beauftragen, wenn er:

- a. sich vergewissert, dass diese die Abklärungen mit derselben Sorgfalt durchführen wie er selbst;
- b. sie über ihre Aufgaben instruiert;
- c. die sorgfältige Durchführung der Abklärungen kontrollieren kann.

² Die Weiterdelegation durch die Beauftragten ist ausgeschlossen.

³ Die Dokumentation der Abklärungen muss beim Finanzintermediär selbst vorliegen.

⁴ Der Finanzintermediär überprüft die Ergebnisse der Abklärungen selber auf ihre Plausibilität.

Art. 20 Zeitpunkt der zusätzlichen Abklärungen

Sobald erhöhte Risiken bei einer Geschäftsbeziehung sichtbar werden, leitet der Finanzintermediär die zusätzlichen Abklärungen unverzüglich in die Wege und führt sie so rasch als möglich durch.

Art. 21 Aufnahme von Geschäftsbeziehungen mit erhöhten Risiken

Die Aufnahme von Geschäftsbeziehungen mit erhöhten Risiken bedarf der Zustimmung einer vorgesetzten Person oder Stelle.

Art. 22 Verantwortung des obersten Geschäftsführungsorgans

¹ Das oberste Geschäftsführungsorgan oder mindestens eines seiner Mitglieder entscheidet über:

- a. die Aufnahme von Geschäftsbeziehungen mit politisch exponierten Personen und alljährlich über deren Weiterführung;
- b. die Anordnung regelmässiger Kontrollen aller Geschäftsbeziehungen mit erhöhten Risiken und ihrer Überwachung und Auswertung.

² Finanzintermediäre mit einem sehr umfangreichen Vermögensverwaltungsgeschäft und mehrstufigen hierarchischen Strukturen können diese Verantwortung der Leitung einer Unternehmenseinheit übertragen.

6. Abschnitt: Dokumentationspflichten

Art. 23 Verfügbarkeit von Informationen

Der Finanzintermediär organisiert seine Dokumentation so, dass er in der Lage ist, den Strafverfolgungsbehörden oder anderen berechtigten Stellen innert angemessener Frist unter Beilage der nötigen Dokumente Auskunft darüber zu geben, ob ein Unternehmen oder eine Person:

- a. Vertragspartei oder wirtschaftlich Berechtigter ist;
- b. ein Kassageschäft getätigt hat, welches die Identifizierung der betroffenen Personen verlangt;
- c. eine dauernde Vollmacht über ein Konto oder Depot besitzt, soweit sie nicht bereits aus einem öffentlichen Register ersichtlich ist.

7. Abschnitt: Verhalten bei Hinweisen auf Geldwäscherei und Verbindungen zu terroristischen Organisationen

Art. 24 Meldung bei Aufnahme von Geschäftsbeziehungen

Bricht der Finanzintermediär Verhandlungen zur Aufnahme einer Geschäftsbeziehung wegen eines offensichtlich begründeten Verdachts auf Geldwäscherei oder auf eine Verbindung zu einer terroristischen oder anderen kriminellen Organisation ab, so erstattet er unverzüglich eine Meldung an die Meldestelle für Geldwäscherei.

Art. 25 Verbindungen zu einer terroristischen Organisation

Weist die Abklärung des Hintergrundes ungewöhnlicher Transaktionen auf eine Verbindung zu einer terroristischen Organisation hin, so erstattet der Finanzintermediär unverzüglich eine Meldung an die Meldestelle für Geldwäscherei.

Art. 26 Verhalten bei fehlender Behördenverfügung

Erhält der Finanzintermediär nach einer Meldung von den Strafverfolgungsbehörden innerhalb der gesetzlichen Frist von fünf Bankwerktagen keine Verfügung, welche die Sperre der Vermögenswerte aufrechterhält, kann er nach eigenem Ermessen entscheiden, ob und in welchem Rahmen er die Geschäftsbeziehung weiterführen will.

Art. 27 Zweifelhafte Geschäftsbeziehungen und Melderecht

¹ Hat ein Finanzintermediär keinen begründeten Verdacht auf Geldwäscherei, aber Wahrnehmungen gemacht, die darauf schliessen lassen, dass Vermögenswerte aus einem Verbrechen herrühren, so kann er diese gestützt auf das Melderecht von Artikel 305^{ter} Absatz 2 des Strafgesetzbuches³ den Strafverfolgungsbehörden und der Meldestelle für Geldwäscherei melden.

² Der Finanzintermediär prüft die Ausübung seines Melderechts insbesondere bei Geschäftsbeziehungen mit bedeutenden Vermögenswerten und dokumentiert das Resultat der Prüfung.

³ SR 311.0

Art. 28 Abbruch zweifelhafter Geschäftsbeziehungen

¹ Bei zweifelhaften Geschäftsbeziehungen, die der Finanzintermediär mangels eines begründeten Verdachts auf Geldwäscherei ohne Meldung abbricht, darf er den Rückzug bedeutender Vermögenswerte nur in einer Form gestatten, welche allenfalls den Strafverfolgungsbehörden erlaubt, die Spur weiterzuverfolgen («paper trail»).

² Der Finanzintermediär darf eine zweifelhafte Geschäftsbeziehung nicht abbrechen oder den Abzug bedeutender Vermögenswerte nicht zulassen, wenn konkrete Anzeichen bestehen, dass behördliche Sicherstellungsmassnahmen unmittelbar bevorstehen.

Art. 29 Weiterführung zweifelhafter Geschäftsbeziehungen

Führt der Finanzintermediär eine zweifelhafte Geschäftsbeziehung weiter, so hat er sie genau zu überwachen und auf Anhaltspunkte für Geldwäscherei (Anhang) zu überprüfen.

Art. 30 Information der Bankenkommission

Der Finanzintermediär informiert die Bankenkommission über Meldungen an die Meldestelle, die Geschäftsbeziehungen mit bedeutenden Vermögenswerten betreffen, oder wenn auf Grund der Umstände anzunehmen ist, dass der Fall, der zur Meldung führte, Auswirkungen auf den Ruf des Finanzintermediärs oder des Finanzplatzes haben könnte.

8. Abschnitt: Revision

Art. 31

Die externen Revisionsstellen der Finanzintermediäre sowie der von der Bankenkommission nach Artikel 2 Absatz 2 beaufsichtigten Gruppengesellschaften prüfen die Einhaltung dieser Verordnung und nehmen dazu im Revisionsbericht Stellung.

9. Abschnitt: Schlussbestimmungen

Art. 32 Übergangsbestimmungen

¹ Die Finanzintermediäre müssen bis zum 30. Juni 2004 die sich aus den Artikeln 3, 6–13, 15 und 17–22 ergebenden Anforderungen nach dieser Verordnung erfüllen. Die Bankenkommission kann diese Frist auf begründetes Gesuch hin verlängern.

² Die Finanzintermediäre haben bis zum 30. Juni 2004 bestehende Geschäftsbeziehungen mit erhöhten Risiken zu ermitteln und intern zu kennzeichnen. Dazu dürfen sie grundsätzlich auf aktuelle Daten abstellen und brauchen nicht rückwirkend Transaktionen zu analysieren.

³ Die Systeme zur Transaktionsüberwachung nach Artikel 12 dieser Verordnung brauchen nur Transaktionen zu erfassen, welche nach dem 30. Juni 2004 getätigt werden.

⁴ Die Finanzintermediäre haben die Massnahmen und den Zeitplan zur Umsetzung dieser Verordnung von ihren externen Revisionsstellen prüfen zu lassen und der Bankenkommission bis zum 30. September 2003 Bericht zu erstatten.

⁵ Die externen Revisionsstellen haben in ihren Revisionsberichten für das Geschäftsjahr 2004:

- a. darzustellen, wie die Finanzintermediäre diese Verordnung umgesetzt haben;
- b. Stellung zu nehmen, ob diese damit den Anforderungen dieser Verordnung genügen.

⁶ Gruppengesellschaften, welche bei Inkrafttreten dieser Verordnung eine Tätigkeit nach Artikel 2 Absatz 3 des Geldwäschereigesetzes ausüben und sich nach Artikel 2 Absatz 2 dieser Verordnung der Aufsicht durch die Bankenkommission unterstellen wollen oder auf Grund des Rundschreibens 98/1 der Bankenkommission bereits unterstellt sind, haben bis zum 30. September 2003 der Bankenkommission ein begründetes Gesuch zu stellen. Die Gesuche können zentral durch die Finanzgruppe erfolgen.

Art. 33 Inkrafttreten

Diese Verordnung tritt am 1. Juli 2003 in Kraft.

18. Dezember 2002

Im Namen der Eidgenössischen
Bankenkommission

Der Präsident: Kurt Hauri

Der Direktor: Daniel Zuberbühler

Anhaltspunkte für Geldwäscherei

I. Bedeutung der Anhaltspunkte

A1 Die nachfolgend aufgeführten Anhaltspunkte, die auf Geldwäscherei hindeuten können, dienen in erster Linie der Sensibilisierung der Finanzintermediäre. Sie geben Hinweise auf Geschäftsbeziehungen oder Transaktionen mit erhöhten Risiken. Die einzelnen Anhaltspunkte dürften jeweils für sich allein in der Regel noch keinen ausreichenden Verdacht für das Vorliegen einer strafbaren Geldwäschereitransaktion begründen, aber das Zusammentreffen mehrerer dieser Elemente kann auf Geldwäscherei hinweisen.

A2 Erklärungen des Kunden über die Hintergründe solcher Transaktionen sind auf ihre Plausibilität hin zu überprüfen. Wesentlich ist dabei, dass nicht jede Erklärung des Kunden (z.B. steuerliche oder devisenrechtliche Beweggründe) unbesehen akzeptiert werden kann.

II. Allgemeine Anhaltspunkte

Besondere Risiken im Hinblick auf Geldwäscherei beinhalten Transaktionen:

A3 deren Konstruktion auf einen widerrechtlichen Zweck hindeutet, deren wirtschaftlicher Zweck nicht erkennbar ist oder die sogar als wirtschaftlich unsinnig erscheinen;

A4 bei denen Vermögenswerte kurz nach ihrem Eingang beim Finanzintermediär wieder abgezogen werden (Durchlaufkonti), sofern sich aus der Geschäftstätigkeit des Kunden kein plausibler Grund für diesen sofortigen Abzug ergibt;

A5 bei denen es unerfindlich ist, warum der Kunde gerade diesen Finanzintermediär oder diese Geschäftsstelle für seine Geschäfte ausgewählt hat;

A6 die dazu führen, dass ein bisher weitgehend inaktives Konto sehr aktiv wird, ohne dass hierfür ein plausibler Grund ersichtlich ist;

A7 die sich mit den Kenntnissen und Erfahrungen des Finanzintermediärs über den Kunden und über den Zweck der Geschäftsbeziehung nicht vereinbaren lassen.

A8 Sodann ist grundsätzlich jeder Kunde verdächtig, welcher dem Finanzintermediär falsche oder irreführende Auskünfte erteilt oder ihm ohne plausiblen Grund für die Geschäftsbeziehung notwendige und für die betreffende Tätigkeit übliche Auskünfte und Unterlagen verweigert.

A8^{bis} Einen Grund zu Verdacht kann bilden, wenn ein Kunde regelmässig Überweisungen erhält, welche von einer Bank ausgehen, die in einem von der «Financial Action Task Force (FATF)» als nicht kooperativ betrachteten Land ansässig ist, oder wenn ein Kunde wiederholt Überweisungen in ein solches Land veranlasst.

III. Einzelne Anhaltspunkte

1. Kassageschäfte

A9 Wechseln eines grösseren Betrages von Banknoten (ausländische und inländische) mit kleinem Nennwert in solche mit grossem Nennwert;

A10 Geldwechsel in wesentlichem Umfang ohne Verbuchung auf einem Kundenkonto;

A11 Einlösung grösserer Beträge mittels Checks einschliesslich Travellerchecks;

A12 Kauf oder Verkauf grösserer Mengen von Edelmetallen durch Laufkunden;

A13 Kauf von Bankchecks in wesentlichem Umfang durch Laufkunden;

A14 Überweisungsaufträge ins Ausland durch Laufkunden, ohne dass ein legitimer Grund ersichtlich ist;

A15 Mehrmaliger Abschluss von Kassageschäften knapp unterhalb der Identifikationslimite;

A16 Erwerb von Inhaberpapieren mittels physischer Lieferung.

2. Bankkonti und -depots

A17 Häufige Abhebungen grösserer Bargeldbeträge, ohne dass sich aus der Geschäftstätigkeit des Kunden ein Grund hierfür finden lässt;

A18 Rückgriff auf Finanzierungsmittel, welche zwar im internationalen Handel üblich sind, deren Gebrauch jedoch im Widerspruch zur bekannten Tätigkeit des Kunden steht;

A19 Konti mit starken Kontobewegungen, obwohl diese Konti normalerweise nicht oder nur wenig benützt werden;

A20 Wirtschaftlich unsinnige Struktur der Geschäftsbeziehungen eines Kunden zur Bank (grosse Anzahl Konti beim gleichen Institut, häufige Verschiebungen zwischen verschiedenen Konti, übertriebene Liquiditäten usw.);

A21 Stellung von Sicherheiten (Pfänder, Bürgschaften) durch der Bank unbekannte Dritte, welche in keiner erkennbar engen Beziehung zum Kunden stehen und für deren Stellung kein plausibler Grund ersichtlich ist;

A22 Überweisungen an eine andere Bank ohne Angabe des Empfängers;

A23 Annahme von Geldüberweisungen anderer Banken ohne Angabe des Namens oder der Nummer des Kontos des Begünstigten oder des Auftraggebers;

A24 Wiederholte Überweisungen in wesentlichem Umfange ins Ausland mit der Anweisung, dass der Betrag dem Empfänger bar ausbezahlen sei;

A25 Grössere und häufige Überweisungen von und nach Drogenproduktionsländern;

A26 Stellung von Bürgschaften oder Bankgarantien zur Sicherung von nicht marktkonformen Darlehen unter Dritten;

A27 Bareinzahlungen einer grossen Anzahl verschiedener Personen auf ein einzelnes Konto;

A28 Unerwartete Rückzahlung eines notleidenden Kredites ohne glaubwürdige Erklärung;

A29 Verwendung von Pseudonym- oder Nummernkonti für die Abwicklung kommerzieller Transaktionen von Handels-, Gewerbe- oder Industriebetrieben;

A30 Rückzug von Vermögenswerten, kurz nachdem diese auf das Konto gutgeschrieben wurden (Durchlaufkonto).

3. Treuhandgeschäfte

A31 Treuhandkredite (back-to-back loans) ohne erkennbaren, rechtlich zulässigen Zweck;

A32 Treuhänderisches Halten von Beteiligungen an nicht börsenkotierten Gesellschaften, in deren Tätigkeit die Bank keinen Einblick nehmen kann.

4. Andere

A33 Versuch des Kunden, den vom Finanzintermediär angestrebten persönlichen Kontakt zu vermeiden.

IV. Besonders verdächtige Anhaltspunkte

A34 Wunsch des Kunden, ohne dokumentarische Spur («paper trail») Konten zu schliessen und neue Konti in seinem oder im Namen seiner Familienangehörigen zu eröffnen;

A35 Wunsch des Kunden nach Quittungen für Barabhebungen oder Auslieferungen von Wertschriften, welche in Tat und Wahrheit nicht getätigt wurden oder bei welchen die Vermögenswerte sogleich wieder beim gleichen Institut hinterlegt wurden;

A36 Wunsch des Kunden, Zahlungsaufträge unter Angabe eines unzutreffenden Auftraggebers auszuführen;

A37 Wunsch des Kunden, dass gewisse Zahlungen nicht über seine Konti, sondern über Nostro-Konti des Finanzintermediärs bzw. über Konti Pro-Diverse laufen;

A38 Wunsch des Kunden, der wirtschaftlichen Realität nicht entsprechende Kreditdeckungen anzunehmen oder auszuweisen oder treuhänderische Kredite unter Ausweis einer fiktiven Deckung zu gewähren;

A39 Strafverfahren gegen den Kunden des Finanzintermediärs wegen Verbrechen, Korruption oder Missbrauches öffentlicher Gelder.

Ordonnance de la Commission fédérale des banques en matière de lutte contre le blanchiment d'argent (Ordonnance de la CFB sur le blanchiment d'argent, OBA-CFB)

du 18 décembre 2002

La Commission fédérale des banques,

vu les art. 16, al. 1, et 41 de la loi du 10 octobre 1997 sur le blanchiment d'argent (LBA)¹,

arrête:

Chapitre 1: Dispositions générales

Art. 1 Définitions

¹ Au sens de la présente ordonnance, on entend par:

- a. personnes politiquement exposées:
 1. les personnes suivantes qui occupent des fonctions publiques importantes à l'étranger: les chefs d'Etat ou de gouvernement, les politiciens de haut rang au niveau national, les hauts fonctionnaires de l'administration, de la justice, de l'armée et des partis au niveau national, les plus hauts organes des entreprises étatiques d'importance nationale;
 2. les entreprises et les personnes qui, de manière reconnaissable, sont proches des personnes précitées pour des raisons familiales ou personnelles ou pour des raisons d'affaires;
- b. négociants professionnels de billets de banque: entreprises ou personnes suisses ou étrangères du secteur non-bancaire qui réalisent par leurs opérations d'achat et de vente de billets de banque un chiffre d'affaires ou un revenu importants;
- c. organisations terroristes: organisations criminelles au sens de l'art. 260^{ter} du code pénal²;
- d. sociétés de groupe: les sociétés qui, aux termes des prescriptions en matière de fonds propres, sont comprises dans le périmètre de consolidation d'un intermédiaire financier au sens de l'art. 2, al. 1.

RS 955.022

¹ RS 955.0

² RS 311.0

Art. 2 *Champ d'application*

¹ La présente ordonnance s'applique aux intermédiaires financiers au sens de l'art. 2, al. 2, let. a, b et d, LBA, à l'exception des directions de fonds de placement lorsque les obligations résultant de la présente ordonnance et de la loi sur le blanchiment d'argent sont assumées par la banque dépositaire.

² Une société suisse appartenant au même groupe qu'un intermédiaire financier au sens de l'al. 1 peut, à sa requête, être assujettie à la surveillance de la Commission fédérale des banques (ci-après: commission des banques) en ce qui concerne l'observation des obligations résultant de la présente ordonnance, dans la mesure où:

- a. elle exerce une activité financière au sens de l'art. 2, al. 3, LBA;
- b. elle satisfait aux conditions de l'art. 14, al. 2, LBA;
- c. elle reconnaît que la commission des banques est habilitée à prononcer à son égard des mesures au sens des art. 19 et 20 LBA;
- d. le groupe garantit qu'il contrôlera que la présente ordonnance est respectée et s'emploiera à la faire appliquer;
- e. le groupe garantit qu'il chargera ses réviseurs externes de contrôler que la présente ordonnance est respectée et de se déterminer à ce sujet dans le rapport de révision du groupe, pour chacune des sociétés du groupe concernées prise séparément.

³ La commission des banques publie une liste des sociétés de groupe dont elle assure la surveillance en vertu de l'al. 2.

Art. 3 *Succursales et sociétés de groupe à l'étranger*

¹ L'intermédiaire financier veille à ce que ses succursales à l'étranger ainsi que les sociétés étrangères de son groupe déployant une activité dans le secteur financier se conforment aux principes fondamentaux de la présente ordonnance.

² Il informe la commission des banques:

- a. lorsque des prescriptions locales excluent l'application des principes fondamentaux de la présente ordonnance, ou
- b. lorsqu'il en résulte pour lui un désavantage concurrentiel sérieux.

³ La communication de transactions ou de relations d'affaires suspectes et, le cas échéant, le blocage des avoirs sont régis par les dispositions du pays d'accueil.

Chapitre 2: Principes

Art. 4 Interdiction de l'acceptation de valeurs patrimoniales provenant de la corruption et d'autres crimes

¹ Il est interdit à l'intermédiaire financier d'accepter des valeurs patrimoniales dont il sait ou doit présumer qu'elles proviennent d'un crime, même si celui-ci a été commis à l'étranger.

² Sont notamment considérées comme provenant d'un crime, les valeurs patrimoniales qui proviennent de la corruption, d'un détournement de fonds publics, d'un abus d'autorité ou d'une gestion déloyale des intérêts publics.

³ L'acceptation par négligence de valeurs patrimoniales provenant d'un crime peut remettre en question la garantie d'une activité irréprochable exigée de l'intermédiaire financier.

Art. 5 Interdiction de relations d'affaires avec des organisations criminelles ou terroristes

L'intermédiaire financier ne doit entretenir aucune relation d'affaires avec des entreprises ou des personnes dont il sait ou doit présumer qu'elles constituent une organisation terroriste ou une organisation criminelle d'un autre type, qu'elles sont membres d'une telle organisation, qu'elles la soutiennent ou qu'elles la financent.

Art. 6 Relations avec des banques correspondantes

¹ Les dispositions de la présente ordonnance s'appliquent également aux relations avec des banques correspondantes.

² L'intermédiaire financier ne doit entretenir aucune relation d'affaires avec des banques qui n'ont pas de présence physique dans l'Etat selon le droit duquel elles sont organisées, à moins qu'elles ne fassent partie d'un groupe financier faisant l'objet d'une surveillance consolidée adéquate.

Chapitre 3: Mesures organisationnelles

Art. 7 Relations d'affaires comportant des risques accrus

¹ L'intermédiaire financier fixe les critères signalant la présence de risques juridiques et de risques de réputation accrus.

² Entrent notamment en considération, selon le domaine d'activité de l'intermédiaire financier, les critères suivants:

- a. le siège ou le domicile du cocontractant et de l'ayant droit économique ou leur nationalité;
- b. la nature et le lieu de l'activité commerciale du cocontractant et de l'ayant droit économique;
- c. l'absence de rencontre avec le cocontractant ainsi qu'avec l'ayant droit économique;
- d. le type de prestations ou de produits sollicités;
- e. l'importance des valeurs patrimoniales remises;
- f. l'importance des entrées et des sorties de valeurs patrimoniales;
- g. le pays d'origine ou de destination de paiements fréquents.

³ Les relations d'affaires avec des personnes politiquement exposées doivent être considérées dans tous les cas comme comportant des risques accrus.

⁴ L'intermédiaire financier détermine les relations d'affaires comportant des risques accrus en vertu des al. 2 et 3 et les désigne comme telles pour l'usage interne.

Art. 8 Transactions présentant des risques accrus

¹ L'intermédiaire financier fixe des critères de détection des transactions présentant des risques juridiques et des risques de réputation accrus.

² Entrent notamment en considération, selon le domaine d'activité de l'intermédiaire financier, les critères suivants:

- a. l'importance des entrées et sorties de valeurs patrimoniales;
- b. l'existence de divergences significatives par rapport à la nature, au volume ou à la fréquence des transactions pratiquées habituellement dans le cadre de la relation d'affaires;

- c. l'existence de divergences significatives par rapport à la nature, au volume ou à la fréquence des transactions pratiquées habituellement dans le cadre de relations d'affaires comparables.
- ³ Sont considérées dans tous les cas comme présentant des risques accrus, les transactions:
- a. dans le cadre desquelles, au début d'une relation d'affaires, des valeurs patrimoniales d'une contre-valeur supérieure à 100 000 francs sont apportées physiquement en une fois ou de manière échelonnée;
 - b. qui présentent des indices de blanchiment (annexe).

Art. 9 Gestion globale des risques juridiques et des risques de réputation

¹ L'intermédiaire financier qui possède des succursales à l'étranger ou dirige un groupe financier comprenant des sociétés étrangères, doit déterminer, limiter et contrôler de manière globale les risques juridiques et les risques de réputation liés au blanchiment d'argent et au financement du terrorisme auxquels il est exposé.

² Il doit s'assurer que:

- a. les organes de contrôle internes et les réviseurs externes du groupe disposent, en cas de besoin, d'un accès aux informations concernant les relations d'affaires de toutes les sociétés du groupe. Ni la constitution d'une banque de données centralisée des cocontractants et des ayants droit économiques au niveau du groupe, ni l'accès centralisé des organes de contrôle internes du groupe aux banques de données locales n'est obligatoire;
- b. les sociétés du groupe mettent à la disposition des organes compétents du groupe les informations nécessaires à la gestion globale des risques juridiques et des risques de réputation.

³ Lorsqu'un intermédiaire financier constate que l'accès aux informations relatives aux cocontractants ou aux ayants droit économiques est, dans certains pays, exclu ou sérieusement entravé pour des motifs d'ordre juridique ou pratique, il en informe sans délai la commission des banques.

⁴ L'intermédiaire financier qui fait partie d'un groupe financier suisse ou international garantit aux organes de contrôle internes ou aux réviseurs externes du groupe l'accès, en cas de besoin, aux informations concernant des relations d'affaires déterminées, dans la mesure nécessaire à la gestion globale des risques juridiques et des risques de réputation.

Art. 10 Directives internes en matière de lutte contre le blanchiment

¹ L'intermédiaire financier émet des directives internes en matière de lutte contre le blanchiment et les communique aux conseillers à la clientèle ainsi qu'à tous les autres collaborateurs concernés.

² Il y règle en particulier:

- a. les critères applicables à la détermination de relations d'affaires comportant des risques accrus selon l'art. 7;
- b. les critères applicables à la détection des transactions présentant des risques accrus selon l'art. 8, al. 1 et 2;
- c. la manière dont il détermine, limite et contrôle ces risques accrus;
- d. les principes applicables au système de surveillance des transactions selon l'art. 12;
- e. les cas dans lesquels le service interne de lutte contre le blanchiment doit être consulté et la direction informée à son plus haut niveau;
- f. les principes régissant la formation des collaborateurs;
- g. la politique de l'entreprise en ce qui concerne les personnes politiquement exposées;
- h. la compétence pour les communications au Bureau de communication en matière de blanchiment d'argent;
- i. les montants limites selon les art. 7, al. 2, let. e et f, et art. 8, al. 2, let. a.

³ Les directives doivent être émises par le conseil d'administration ou par la direction à son plus haut niveau.

Art. 11 Formation du personnel

L'intermédiaire financier veille à ce que les conseillers à la clientèle et tous les autres collaborateurs concernés reçoivent une formation régulière. Cette formation couvre les aspects essentiels pour eux de la lutte contre le blanchiment d'argent.

Art. 12 Systèmes de surveillance des transactions

¹ L'intermédiaire financier veille à la mise en place d'une surveillance efficace des transactions et utilise un système informatique aidant à détecter les transactions présentant des risques accrus selon l'art. 8, al. 1, al. 2 et al. 3, let. a.

² Les transactions détectées par le système de surveillance doivent être examinées dans un délai raisonnable. Au besoin, des clarifications complémentaires selon l'art. 17 doivent être entreprises.

³ Les intermédiaires financiers ayant peu de cocontractants et d'ayants droit économiques ou effectuant peu de transactions peuvent renoncer à l'usage d'un système de surveillance informatisé, dans la mesure où ils chargent leurs réviseurs externes de procéder à un contrôle annuel approfondi de leur surveillance des transactions.

Art. 13 Service interne de lutte contre le blanchiment

¹ L'intermédiaire financier doit désigner une ou plusieurs personnes qualifiées qui constituent le service interne de lutte contre le blanchiment. Ce service fournit le soutien et les conseils nécessaires aux responsables des lignes hiérarchiques et à la direction pour la mise en œuvre de la présente ordonnance, sans toutefois dégager ceux-ci de leur responsabilité en la matière.

² Le service interne de lutte contre le blanchiment:

- a. prépare les directives internes en matière de lutte contre le blanchiment;
- b. surveille l'exécution des directives internes en matière de lutte contre le blanchiment en accord avec l'organe de révision interne, les réviseurs externes et les responsables des lignes hiérarchiques;

- c. planifie et surveille la formation interne en matière de lutte contre le blanchiment;
- d. définit les paramètres du système de surveillance des transactions visé à l'art. 12;
- e. fait procéder à l'examen des annonces générées par le système de surveillance des transactions;
- f. fait procéder ou procède lui-même aux clarifications complémentaires visées à l'art. 17;
- g. s'assure que l'organe de direction compétent pour décider de l'admission ou de la poursuite de relations d'affaires selon l'art. 22, al. 1, reçoit l'information nécessaire pour prendre sa décision.

³ L'intermédiaire financier peut également, sous sa responsabilité, confier à des spécialistes externes les tâches du service interne de lutte contre le blanchiment lorsque:

- a. en raison de sa taille ou de son organisation, il n'est pas en mesure de mettre sur pied son propre service spécialisé, ou
- b. la création d'un tel service ne serait pas appropriée.

Chapitre 4: Obligations de diligence générales

Art. 14 Vérification de l'identité du cocontractant et identification de l'ayant droit économique

¹ Les dispositions sur la vérification de l'identité des cocontractants et l'identification des ayants droit économiques de la Convention du 2 décembre 2002 relative à l'obligation de diligence des banques (CDB 2003), conclue entre les banques et l'Association suisse des banquiers, sont applicables à tous les intermédiaires financiers.

² La violation de la CDB 2003 peut remettre en question la garantie d'une activité irréprochable exigée de l'intermédiaire financier.

Art. 15 Indication des donneurs d'ordre lors de virements

¹ Pour tous les virements effectués vers l'étranger, l'intermédiaire financier indique le nom, le numéro de compte et le domicile du cocon-

tractant donneur d'ordre ou le nom et un numéro d'identification de celui-ci.

² L'intermédiaire financier peut renoncer à faire figurer ces indications pour des motifs légitimes, notamment en cas d'ordre permanent. Il doit clarifier ces motifs et les documenter.

Art. 16 Commerce professionnel de billets de banque

¹ Le commerce professionnel de billets de banque n'est autorisé qu'avec des négociants en billets de banque qui remplissent les critères d'une relation de correspondance bancaire digne de confiance.

² Avant d'établir la relation, l'intermédiaire financier doit se renseigner sur l'activité commerciale du négociant en billets de banque et se procurer des renseignements commerciaux et des références.

³ L'intermédiaire financier fixe des limites de chiffre d'affaires et de crédit pour son commerce professionnel de billets de banque dans sa totalité et pour chaque partie contractante. Il doit réexaminer ces limites au moins une fois par an et veiller en permanence à ce qu'elles soient respectées.

⁴ L'intermédiaire financier qui pratique le commerce de billets de banques de manière professionnelle élabore des directives à cet effet. Celles-ci doivent en principe être adoptées par la direction à son plus haut niveau.

Chapitre 5: Obligations de diligence accrues

Art. 17 Clarifications complémentaires en cas de risques accrus

¹ L'intermédiaire financier entreprend, dans une mesure proportionnée aux circonstances, les clarifications complémentaires relatives aux relations ou transactions présentant des risques accrus.

² Selon les circonstances, il y a lieu d'établir notamment:

- a. si le cocontractant est l'ayant droit économique des valeurs patrimoniales remises;
- b. quelle est l'origine des valeurs patrimoniales remises;
- c. à quelle fin les valeurs patrimoniales prélevées sont utilisées;

- d. si les versements entrants importants sont plausibles;
- e. quelle est l'origine de la fortune du cocontractant et de l'ayant droit économique;
- f. quelle activité professionnelle ou commerciale exercent le cocontractant et l'ayant droit économique;
- g. si le cocontractant ou l'ayant droit économique sont des personnes politiquement exposées;
- h. pour les personnes morales: par qui elles sont contrôlées.

Art. 18 Moyens de clarification

¹ Selon les circonstances, les clarifications comprennent notamment:

- a. la prise de renseignements écrits ou oraux auprès des cocontractants ou des ayants droit économiques;
- b. des visites des lieux où les cocontractants et les ayants droit économiques conduisent leurs affaires;
- c. une consultation des sources et des banques de données accessibles au public;
- d. le cas échéant, des renseignements auprès de personnes dignes de confiance.

² Les clarifications sont effectuées dans le respect de la sphère privée des personnes concernées.

³ L'intermédiaire financier vérifie si les résultats des clarifications sont plausibles et les documente.

Art. 19 Délégation des clarifications complémentaires à des tiers

¹ L'intermédiaire financier peut, sur la base d'une convention écrite, charger des personnes ou des entreprises d'effectuer les clarifications complémentaires, dans la mesure où:

- a. il s'assure que ces mandataires exécutent les clarifications avec la même diligence qu'il y mettrait lui-même;
- b. il instruit ces mandataires en vue de l'accomplissement de leurs tâches;

c. il peut contrôler que les clarifications sont effectuées avec diligence.

² La sous-délégation par le mandataire est interdite.

³ La documentation relative aux clarifications doit être déposée auprès de l'intermédiaire financier lui-même.

⁴ L'intermédiaire financier examine lui-même la plausibilité des résultats des clarifications.

Art. 20 Moment des clarifications complémentaires

L'intermédiaire financier entreprend les clarifications complémentaires dès que des risques accrus se font jour dans une relation d'affaires et mène ces clarifications à bien le plus rapidement possible.

Art. 21 Admission de relations d'affaires comportant des risques accrus

L'admission de relations d'affaires comportant des risques accrus nécessite l'accord d'une personne ou d'un organe supérieur.

Art. 22 Responsabilité de la direction à son plus haut niveau

¹ La direction à son plus haut niveau ou l'un de ses membres au moins décide:

- a. de l'admission et, tous les ans, de la poursuite des relations d'affaires avec des personnes politiquement exposées;
- b. de la mise en œuvre, de la surveillance et de l'évaluation des contrôles réguliers de toutes les relations d'affaires comportant des risques accrus.

² Les intermédiaires financiers ayant une activité de gestion de fortune très importante et des structures comportant de nombreux niveaux hiérarchiques peuvent déléguer cette responsabilité à la direction d'une unité d'affaires.

Chapitre 6: Devoirs de documentation

Art. 23 Disponibilité de l'information

L'intermédiaire financier organise sa documentation de façon à être en mesure d'indiquer dans un délai raisonnable, documents à l'appui, aux autorités de poursuite pénale ou à d'autres autorités habilitées si une entreprise ou personne:

- a. est un cocontractant ou un ayant droit économique;
- b. a effectué une opération de caisse exigeant la vérification de l'identité des personnes concernées;
- c. dispose d'une procuration durable sur un compte ou un dépôt, dans la mesure où celle-ci ne ressort pas déjà d'un registre officiel.

Chapitre 7: Comportement en présence d'indices de blanchiment ou de liens avec des organisations terroristes

Art. 24 Communication lors de l'établissement d'une relation d'affaires

Lorsque l'intermédiaire financier rompt des négociations visant à établir une relation d'affaires en raison de soupçons fondés manifestes de blanchiment ou de lien avec une organisation terroriste ou une organisation criminelle d'un autre type, il adresse sans retard une communication au Bureau de communication en matière de blanchiment d'argent.

Art. 25 Liens avec une organisation terroriste

Lorsque la clarification de l'arrière-plan économique de transactions inhabituelles révèle un lien avec une organisation terroriste, l'intermédiaire financier adresse sans tarder une communication au Bureau de communication en matière de blanchiment d'argent.

Art. 26 Comportement en l'absence de décision des autorités

Si, dans le délai légal de cinq jours bancaires ouvrables après une communication, l'intermédiaire financier ne reçoit pas de décision des autorités de poursuite pénale maintenant le blocage des valeurs patri-

moniales, il peut apprécier librement si et dans quelle mesure il entend poursuivre la relation d'affaires.

Art. 27 Doutes sur la qualité d'une relation d'affaires et droit de communication

¹ Lorsqu'un intermédiaire financier n'a pas de soupçons fondés de blanchiment au sujet d'une relation d'affaires mais possède des indices fondant le soupçon que des valeurs patrimoniales proviennent d'un crime, il peut faire usage de son droit de communication au sens de l'art. 305^{ter}, al. 2, du code pénal³, et communiquer ces indices aux autorités de poursuite pénale et au Bureau de communication en matière de blanchiment d'argent.

² L'intermédiaire financier examine l'exercice de son droit de communication en particulier dans le cas de relations d'affaires comportant d'importantes valeurs patrimoniales. Il documente le résultat de cet examen.

Art. 28 Rupture de relations d'affaires douteuses

¹ Lorsqu'un intermédiaire financier met un terme à une relation d'affaires douteuse sans procéder à une communication faute de disposer de soupçons fondés de blanchiment, il ne peut autoriser le retrait d'importantes valeurs patrimoniales que sous une forme qui permette aux autorités de poursuite pénale, le cas échéant, d'en suivre la trace («paper trail»).

² L'intermédiaire financier ne doit pas rompre une relation d'affaires douteuse ni autoriser le retrait de montants importants lorsqu'il existe des signes concrets de l'imminence de mesures de sûreté d'une autorité.

Art. 29 Poursuite de relations d'affaires douteuses

L'intermédiaire financier qui décide de poursuivre une relation d'affaires douteuse est tenu de la maintenir sous surveillance stricte et de l'examiner à la lumière des indices de blanchiment (annexe).

³ RS 311.0

Art. 30 Information de la commission des banques

L'intermédiaire financier informe la commission des banques des communications adressées au Bureau de communication qui concernent des relations d'affaires comportant d'importantes valeurs patrimoniales ou lorsqu'il y a lieu de penser, au vu des circonstances, que l'affaire ayant entraîné la communication aura des conséquences sur la réputation de l'intermédiaire financier ou sur celle de la place financière.

Chapitre 8: Révision

Art. 31

Les réviseurs externes de l'intermédiaire financier ainsi que ceux des sociétés de groupe soumises à la surveillance de la commission des banques selon l'art. 2, al. 2, contrôlent que la présente ordonnance est respectée et se déterminent à ce sujet dans leur rapport de révision.

Chapitre 9: Dispositions finales

Art. 32 Dispositions transitoires

¹ Les intermédiaires financiers doivent se conformer aux exigences des art. 3, 6 à 13, 15 et 17 à 22 le 30 juin 2004 au plus tard. La commission des banques peut prolonger ce délai sur requête motivée.

² Les intermédiaires financiers doivent déterminer les relations d'affaires comportant des risques accrus et les désigner comme telles pour l'usage interne le 30 juin 2004 au plus tard. En principe, ils peuvent se fonder sur des données actuelles et ne sont pas tenus d'analyser rétroactivement les transactions.

³ Les systèmes de surveillance des transactions visés à l'art. 12 ne doivent porter que sur les transactions effectuées après le 30 juin 2004.

⁴ Les intermédiaires financiers font examiner les mesures et le calendrier de mise en œuvre de la présente ordonnance par leurs réviseurs externes et déposent un rapport y relatif à la commission des banques le 30 septembre 2003 au plus tard.

⁵ Dans leur rapport de révision pour l'année 2004, les réviseurs externes doivent:

- a. exposer la manière dont la présente ordonnance a été mise en œuvre par les intermédiaires financiers;
- b. indiquer si ces derniers satisfont ainsi aux exigences de la présente ordonnance.

⁶ Les sociétés d'un groupe qui, lors de l'entrée en vigueur de la présente ordonnance, exercent une activité au sens de l'art. 2, al. 3, LBA, et qui veulent être assujetties à la surveillance de la commission des banques en vertu de l'art. 2, al. 2, de la présente ordonnance ou le sont déjà en application de la circulaire 98/1 de la commission des banques doivent déposer une requête motivée auprès de cette dernière le 30 septembre 2003 au plus tard. Les requêtes peuvent être soumises par le groupe financier de manière centralisée.

Art. 33 Entrée en vigueur

La présente ordonnance entre en vigueur au 1^{er} juillet 2003.

18 décembre 2002

Au nom de la Commission fédérale
des banques:

Le président, Kurt Hauri
Le directeur, Daniel Zuberbühler

Indices de blanchiment d'argent

I. Importance des indices

A1 Les indices de blanchiment énumérés ci-dessous servent avant tout à sensibiliser les intermédiaires financiers. Ils permettent de signaler les relations d'affaires ou transactions présentant des risques accrus. Les indices pris séparément ne permettent pas, en règle générale, de fonder un soupçon suffisant de l'existence d'une opération de blanchiment. Cependant, le concours de plusieurs de ces éléments peut en indiquer la présence.

A2 Il faut examiner la plausibilité des explications du client quant à l'arrière-plan économique de telles opérations. A cet égard, il est important que les explications du client (p.ex. raisons fiscales ou raisons se rapportant à la législation sur les devises) ne soient pas acceptées sans examen.

II. Indices généraux

Les transactions présentent des risques particuliers de blanchiment:

A3 lorsque leur construction indique un but illicite, lorsque leur but économique n'est pas reconnaissable, voire lorsqu'elles apparaissent absurdes d'un point de vue économique;

A4 lorsque les valeurs patrimoniales sont retirées peu de temps après avoir été portées en compte (compte de passage), pour autant que l'activité du client ne rende pas plausible un tel retrait immédiat;

A5 lorsque l'on ne parvient pas à comprendre les raisons pour lesquelles le client a choisi précisément cette banque ou ce comptoir pour ses affaires;

A6 lorsqu'elles ont pour conséquence qu'un compte, resté jus-

que-là largement inactif, devient très actif sans que l'on puisse en percevoir une raison plausible;

A7 lorsqu'elles ne sont pas compatibles avec les informations et les expériences de l'intermédiaire financier concernant le client ou le but de la relation d'affaires.

A8 En outre, doit être considéré comme suspect tout client qui donne à l'intermédiaire financier des renseignements faux ou fallacieux ou qui, sans raison plausible, refuse de lui fournir les informations et les documents nécessaires, admis par les usages de l'activité concernée.

A8^{bis} Peut constituer un motif de suspicion, le fait qu'un client reçoive régulièrement des virements en provenance d'une banque établie dans un des pays considéré comme non coopératif par le «Groupe d'Action Financière (GAFI)», ou qu'un client procède de manière répétée à des virements en direction d'un tel pays.

III. Indices particuliers

1. Opérations de caisse

A9 Echange d'un montant important de billets de banque (suisses ou étrangers) en petites coupures contre des grosses coupures.

A10 Opérations de change d'importance, sans comptabilisation sur le compte d'un client.

A11 Encaissement de chèques, chèques de voyage y compris, pour des montants importants.

A12 Achat ou vente de grandes quantités de métaux précieux par des clients occasionnels.

A13 Achat de chèques bancaires pour de gros montants par des clients occasionnels.

A14 Ordres de virement à l'étranger donnés par des clients occasionnels, sans raison légitime apparente.

A15 Conclusion fréquente d'opérations de caisse jusqu'à concurrence de montants juste inférieurs à la limite au-dessus de laquelle l'identification du client est exigée.

A16 Acquisition de titres au porteur avec livraison physique.

2. Opérations en compte ou en dépôt

A17 Retraits fréquents de gros montants en espèces, sans que l'activité du client ne justifie de telles opérations.

A18 Recours à des moyens de financement en usage dans le commerce international, alors que l'emploi de tels instruments est en contradiction avec l'activité connue du client.

A19 Comptes utilisés de manière intensive pour des paiements, alors que lesdits comptes ne reçoivent pas ou reçoivent peu de paiements habituellement.

A20 Structure économiquement absurde des relations d'affaires entre un client et la banque (grand nombre de comptes auprès du même établissement, transferts fréquents entre différents comptes, liquidités excessives, etc.).

A21 Fourniture de garanties (gages, cautions, etc.) par des tiers inconnus de la banque qui ne paraissent pas être en relation étroite avec le client ni avoir de raison plausible de donner de telles garanties.

A22 Virements vers une autre banque sans indication du bénéficiaire.

A23 Acceptation de transferts de fonds d'autres banques sans indication du nom ou du numéro de compte du bénéficiaire ou du donneur d'ordre.

A24 Virements répétés de gros montants à l'étranger avec instruction de payer le bénéficiaire en espèces.

A25 Virements importants et répétés en direction ou en provenance de pays producteurs de drogue.

A26 Fourniture de cautions ou de garanties bancaires à titre de sûreté pour des emprunts entre tiers, non conformes au marché.

A27 Versements en espèces par un grand nombre de personnes différentes sur un seul et même compte.

A28 Remboursement inattendu et sans explications convaincantes d'un crédit compromis.

A29 Utilisation de comptes pseudonymes ou numériques dans l'exécution de transactions commerciales par des entreprises artisanales, commerciales ou industrielles.

A30 Retrait de valeurs patrimoniales peu de temps après que celles-ci ont été portées en compte (compte de passage).

3. Opérations fiduciaires

A31 Crédits fiduciaires (back-to-back loans) sans but licite reconstituable.

A32 Détention fiduciaire de participations dans des sociétés non cotées en bourse, et dont la banque ne peut déterminer l'activité.

4. Autres

A33 Tentatives du client visant à éviter le contact personnel avec l'intermédiaire financier.

IV. Indices qualifiés

A34 Souhait du client de clôturer un compte et d'ouvrir de nouveaux comptes en son nom ou au nom de certains membres de sa famille sans traces dans la documentation de la banque («paper trail»).

A35 Souhait du client d'obtenir quittance pour des retraits au comptant ou des livraisons de titres qui n'ont pas été réellement effectués ou qui ont été immédiatement redéposés dans le même établissement.

A36 Souhait du client d'effectuer des ordres de paiement avec indication d'un donneur d'ordre inexact.

A37 Souhait du client que certains versements soient effectués non pas directement depuis son propre compte, mais par le biais d'un compte Nostro de l'intermédiaire financier ou d'un compte «Divers».

A38 Souhait du client d'accepter ou de faire documenter des garanties ne correspondant pas à la réalité économique ou d'octroyer des crédits à titre fiduciaire sur la base d'une couverture fictive.

A39 Poursuites pénales dirigées contre un client de l'intermédiaire financier pour crime, corruption ou détournement de fonds publics.

Ordinanza della Commissione federale delle banche relativa alla lotta contro il riciclaggio di denaro (Ordinanza CFB sul riciclaggio di denaro, ORD-CFB)

del 18 dicembre 2002

La Commissione federale delle banche,

visti gli articoli 16 capoverso 1 e 41 della legge del 10 ottobre 1997¹ sul riciclaggio di denaro (LRD),

ordina:

Sezione 1: Disposizioni generali

Art. 1 Definizioni

Ai sensi della presente ordinanza si intendono per:

- a. persone politicamente esposte:
 1. le persone che occupano una funzione pubblica preminente all'estero, quali: capi di Stato e di Governo, politici di alto rango a livello nazionale, alti funzionari dell'amministrazione, della giustizia, dell'esercito e dei partiti a livello nazionale, organi superiori delle imprese pubbliche di importanza nazionale,
 2. le imprese e persone che sono riconoscibilmente legate per motivi familiari, personali o d'affari alle persone sopra elencate;
- b. negozianti professionali di biglietti di banca: imprese o persone del settore non bancario svizzero o estero, che realizzano mediante la loro attività di vendita e acquisto di biglietti di banca una cifra d'affari o un reddito importanti;
- c. organizzazioni terroristiche: organizzazioni criminali ai sensi dell'articolo 260^{ter} del Codice penale²;
- d. società del gruppo: società che, secondo i termini delle disposizioni sui fondi propri, sono comprese nel perimetro di consolida-

RS 955.022

¹ RS 955.0

² RS 311.0

zione di un intermediario finanziario ai sensi dell'articolo 2 capoverso 1.

Art. 2 Campo di applicazione

¹ La presente ordinanza si applica agli intermediari finanziari secondo l'articolo 2 capoverso 2 lettere a, b e d LRD, ad eccezione delle direzioni di fondi, quando gli obblighi previsti dalla presente ordinanza e dalla LRD sono assunti dalla banca depositaria.

² Una società svizzera del gruppo comprendente un intermediario finanziario ai sensi del capoverso 1 può, su sua richiesta, essere assoggettata alla sorveglianza della Commissione federale delle banche per quel che concerne l'osservazione degli obblighi derivanti dalla presente ordinanza, nella misura in cui:

- a. essa esercita un'attività finanziaria ai sensi dell'articolo 2 capoverso 3 LRD;
- b. essa adempie alle condizioni previste all'articolo 14 capoverso 2 LRD;
- c. essa riconosce che la Commissione federale delle banche è abilitata a pronunciare nei suoi confronti le misure previste agli articoli 19 e 20 LRD;
- d. il gruppo assicura che controllerà il rispetto della presente ordinanza e che provvederà all'applicazione di quest'ultima;
- e. il gruppo assicura che darà mandato al revisore esterno di controllare il rispetto della presente ordinanza e di prendere posizione in merito nel rapporto di revisione del gruppo, individualmente per ognuna delle società del gruppo coinvolte.

³ La Commissione federale delle banche pubblica un elenco delle società per le quali essa assicura la sorveglianza conformemente al capoverso 2.

Art. 3 Succursali e società del gruppo all'estero

¹ L'intermediario finanziario vigila affinché le sue succursali all'estero

nonché le società estere del suo gruppo attive nel settore finanziario si conformino ai principi fondamentali della presente ordinanza.

² Egli informa la Commissione federale delle banche quando:

- a. le prescrizioni locali escludono l'applicazione dei principi fondamentali della presente ordinanza; oppure
- b. la loro applicazione gli causa un serio svantaggio concorrenziale.

³ La comunicazione di transazioni o di relazioni d'affari sospette nonché l'eventuale blocco degli averi sono regolati dal diritto dello Stato di accoglienza.

Sezione 2: Principi

Art. 4 Divieto di accettazione di valori patrimoniali provenienti dalla corruzione e da altri crimini

¹ L'intermediario finanziario non può accettare i valori patrimoniali di cui sa o deve presumere che provengono da un crimine, anche se questo è stato commesso all'estero.

² Sono segnatamente considerati di origine criminale i valori patrimoniali che provengono dalla corruzione, dalla sottrazione di fondi pubblici, dall'abuso di autorità o dall'infedeltà nella gestione pubblica.

³ L'accettazione per negligenza di valori patrimoniali provenienti da un crimine può mettere in questione la garanzia di un'attività irreprensibile richiesta all'intermediario finanziario.

Art. 5 Divieto di relazioni d'affari con organizzazioni criminali o terroristiche

L'intermediario finanziario non può intrattenere nessuna relazione d'affari con imprese o persone di cui sa o deve presumere che costituiscono un'organizzazione terroristica o un'organizzazione criminale di altro genere o che sono membri di un'organizzazione di questo tipo, la sostengono o la finanziano.

Art. 6 Relazioni con banche corrispondenti

¹ Le disposizioni della presente ordinanza si applicano anche alle relazioni con banche corrispondenti.

² L'intermediario finanziario non può intrattenere relazioni d'affari con banche che non hanno una presenza fisica nello Stato secondo il diritto del quale sono organizzate, ad eccezione delle banche che fanno parte di un gruppo finanziario che è oggetto di una sorveglianza consolidata adeguata.

Sezione 3: Misure di organizzazione

Art. 7 Relazioni d'affari che comportano un rischio superiore

¹ L'intermediario finanziario stabilisce criteri per il riconoscimento di relazioni d'affari che comportano rischi giuridici e rischi di reputazione superiori.

² In funzione dell'attività dell'intermediario finanziario entrano in considerazione segnatamente i criteri seguenti:

- a. sede o domicilio della controparte e dell'avente economicamente diritto oppure la loro nazionalità;
- b. tipo e luogo dell'attività commerciale della controparte e dell'avente economicamente diritto;
- c. l'assenza di un contatto personale con la controparte e con l'avente economicamente diritto;
- d. il tipo di prestazioni o di prodotti richiesti;
- e. l'ammontare dei valori patrimoniali depositati;
- f. l'ammontare dei valori patrimoniali in entrata ed in uscita;
- g. il Paese di origine o di destinazione di pagamenti frequenti.

³ Le relazioni d'affari con persone politicamente esposte sono considerate in ogni caso a rischio superiore.

⁴ L'intermediario finanziario determina le relazioni d'affari che comportano un rischio superiore conformemente ai capoversi 1 e 2 e le designa come tali per l'uso interno.

Art. 8 Transazioni che comportano un rischio superiore

¹ L'intermediario finanziario stabilisce criteri per il riconoscimento di transazioni che comportano rischi giuridici e rischi di reputazione superiori.

² In funzione dell'attività dell'intermediario finanziario entrano in considerazione segnatamente i criteri seguenti:

- a. l'ammontare dei valori patrimoniali in entrata e in uscita;
- b. le divergenze significative del tipo, del volume e della frequenza delle transazioni rispetto alle transazioni normalmente effettuate dalla stessa relazione d'affari;
- c. le divergenze significative del tipo, del volume e della frequenza delle transazioni rispetto alle transazioni normalmente effettuate da relazioni d'affari simili.

³ Sono considerate in ogni caso transazioni che comportano un rischio superiore le transazioni:

- a. mediante le quali all'inizio di una relazione d'affari vengono fisicamente apportati valori patrimoniali per un controvalore superiore a 100 000 franchi in una volta o in modo scaglionato;
- b. che presentano un indizio di riciclaggio di denaro (Allegato).

Art. 9 Sorveglianza globale dei rischi giuridici e di reputazione

¹ L'intermediario finanziario che possiede succursali all'estero oppure dirige un gruppo finanziario che comprende società estere, deve determinare, limitare e controllare in maniera globale i suoi rischi giuridici e dei rischi di reputazione legati al riciclaggio di denaro e al finanziamento del terrorismo.

² Egli deve assicurare che:

- a. gli organi di sorveglianza interni e il revisore esterno del gruppo dispongono, in caso di bisogno, di un accesso alle informazioni concernenti le relazioni d'affari individuali di tutte le società del gruppo. Non è obbligatoria né la costituzione di una banca dati centralizzata delle controparti e degli aventi economicamente diritto a livello del gruppo, né l'accesso centralizzato degli organi di sorveglianza interni del gruppo alle banche dati locali;
- b. le società del gruppo mettono a disposizione degli organi competenti del gruppo le informazioni necessarie alla sorveglianza globale dei rischi giuridici e dei rischi di reputazione.

³ L'intermediario finanziario deve informare immediatamente la Commissione federale delle banche quando constata che l'accesso alle informazioni relative alle controparti o agli aventi economicamente diritto è, in certi Paesi, esclusa o seriamente limitata per motivi di ordine giuridico o pratico.

⁴ L'intermediario finanziario che fa parte di un gruppo finanziario svizzero o estero garantisce agli organi di sorveglianza interni o al revisore esterno del gruppo l'accesso, in caso di bisogno, alle informazioni concernenti determinate relazioni d'affari, nella misura necessaria alla sorveglianza globale dei rischi giuridici e dei rischi di reputazione.

Art. 10 Direttive interne sulla lotta contro il riciclaggio di denaro

¹ L'intermediario finanziario emana direttive interne sulla lotta contro il riciclaggio di denaro e le comunica ai consulenti della clientela nonché a tutti gli altri collaboratori interessati.

² Disciplina segnatamente:

- a. i criteri applicati per la determinazione delle relazioni d'affari che comportano i rischi superiori di cui all'articolo 7;
- b. i criteri applicati per la determinazione delle transazioni che comportano i rischi superiori di cui all'articolo 8 capoversi 1 e 2;
- c. il modo in cui egli determina, limita e sorveglia questi rischi superiori;
- d. i principi di base per la sorveglianza delle transazioni secondo l'articolo 12;
- e. i casi nei quali il servizio interno di lotta contro il riciclaggio di denaro deve essere consultato e la direzione generale deve essere informata;
- f. i principi di base della formazione dei collaboratori;
- g. la politica dell'impresa nei confronti delle persone politicamente esposte;
- h. le competenze per la comunicazione all'Ufficio di comunicazione in materia di riciclaggio di denaro;

i. gli importi limite di cui all'articolo 7 capoverso 2 lettere e e f nonché all'articolo 8 capoverso 2 lettera a.

³ Le direttive sono emanate dal consiglio di amministrazione o dalla direzione generale.

Art. 11 Formazione del personale

L'intermediario finanziario vigila affinché i consulenti della clientela e tutti i collaboratori interessati ricevano periodicamente una formazione sugli aspetti per essi essenziali della lotta contro il riciclaggio.

Art. 12 Sistemi di sorveglianza delle transazioni

¹ L'intermediario finanziario provvede a un'efficiente sorveglianza delle transazioni e gestisce un sistema informatico che lo aiuti a rilevare le transazioni che comportano un rischio superiore conformemente all'articolo 8 capoversi 1, 2 e 3 lettera a.

² Le transazioni rilevate dal sistema di sorveglianza devono essere valutate entro un congruo termine. Se necessario devono essere espletate le chiarificazioni supplementari di cui all'articolo 17.

³ Gli intermediari finanziari con un numero ristretto di controparti e aventi economicamente diritto o quelli che effettuano un numero limitato di transazioni possono rinunciare all'uso di un sistema di sorveglianza informatico, nella misura in cui incaricano il loro revisore esterno di eseguire un controllo annuale approfondito sulla loro sorveglianza delle transazioni.

Art. 13 Servizio interno di lotta contro il riciclaggio di denaro

¹ L'intermediario finanziario nomina una o più persone qualificate che costituiscono il servizio interno di lotta contro il riciclaggio di denaro. Questo servizio fornisce il sostegno e i consigli necessari al responsabile di linea e alla direzione nell'applicazione della presente ordinanza, senza tuttavia liberare questi ultimi dalla loro responsabilità.

² Il servizio interno di lotta contro il riciclaggio di denaro:

- a. prepara le direttive interne sulla lotta contro il riciclaggio di denaro;
 - b. sorveglia, d'accordo con l'organo di revisione interno, il revisore esterno e i responsabili di linea, l'applicazione delle direttive interne sulla lotta contro il riciclaggio di denaro;
 - c. pianifica e sorveglia la formazione interna in materia di lotta contro il riciclaggio di denaro;
 - d. definisce i parametri del sistema di sorveglianza delle transazioni di cui all'articolo 12;
 - e. ordina la valutazione degli annunci generati dal sistema di sorveglianza delle transazioni;
 - f. ordina le chiarificazioni complementari secondo l'articolo 17 o le esegue di persona;
 - g. si assicura che l'organo della direzione competente per decidere l'ammissione o il proseguimento di relazioni d'affari conformemente all'articolo 22 capoverso 1 riceva le informazioni necessarie per la sua decisione.
- ³ L'intermediario finanziario può, sotto la sua responsabilità, incaricare specialisti esterni dei compiti del servizio interno di lotta contro il riciclaggio di denaro, se:
- a. in ragione della sua dimensione o della sua organizzazione, non è in grado di istituire un proprio servizio specializzato; oppure
 - b. l'istituzione di un tale servizio non appare appropriata.

Sezione 4: Obblighi generali di diligenza

Art. 14 Identificazione della controparte e determinazione dell'avente economicamente diritto

¹ Le disposizioni in materia di identificazione della controparte e di determinazione dell'avente economicamente diritto della Convenzione del 2 dicembre 2002 relativa all'obbligo di diligenza delle banche (CDB 2003), conclusa tra le banche e l'Associazione svizzera dei banchieri, sono applicabili a tutti gli intermediari finanziari.

² La violazione della CDB 2003 può mettere in questione la garanzia di un'attività irreprensibile richiesta all'intermediario finanziario.

Art. 15 Indicazioni sull'ordinante negli ordini di bonifico

¹ Per tutti gli ordini di bonifico effettuati verso l'estero l'intermediario finanziario indica il nome, il numero di conto e il domicilio della controparte ordinante oppure il nome di quest'ultima e un numero di identificazione.

² Per motivi legittimi, segnatamente in caso di ordini permanenti, l'intermediario finanziario può rinunciare a indicare tali dati. I motivi devono essere verificati e documentati.

Art. 16 Negozio professionale di biglietti di banca

¹ Il negozio professionale di biglietti di banca è autorizzato solo con negozianti di biglietti di banca che adempiono ai criteri di una relazione di banca di corrispondenza degna di fiducia.

² Prima dell'ammissione di una relazione l'intermediario finanziario deve informarsi sull'attività commerciale del negoziante professionale di biglietti di banca e procurarsi le informazioni commerciali e le referenze.

³ L'intermediario finanziario fissa i limiti di cifra d'affari e di credito per il proprio negozio professionale di biglietti di banca nella sua totalità e per ogni controparte. Egli deve riesaminare questi limiti almeno una volta l'anno e controllarne il rispetto in modo continuo.

⁴ L'intermediario finanziario che pratica il negozio professionale di biglietti di banca emana direttive a questo scopo; di regola tali direttive sono adottate dalla direzione generale.

Sezione 5: Obblighi di diligenza particolari

Art. 17 Chiarificazioni complementari in caso di rischi superiori

¹ In misura proporzionata alle circostanze, l'intermediario finanziario procede a chiarificazioni complementari riguardanti le relazioni e le transazioni che presentano rischi superiori.

² Secondo le circostanze, occorre chiarire segnatamente:

- a. se la controparte è l'avente economicamente diritto dei valori patrimoniali consegnati;
- b. qual è l'origine dei valori patrimoniali consegnati;
- c. a quale scopo i valori patrimoniali prelevati sono utilizzati;
- d. se i versamenti importanti in entrata sono plausibili;
- e. qual è l'origine del patrimonio della controparte e dell'avente economicamente diritto;
- f. qual è l'attività professionale o commerciale esercitata dalla controparte e dall'avente economicamente diritto;
- g. se la controparte o l'avente economicamente diritto sono politicamente esposti;
- h. per le persone giuridiche: chi le controlla.

Art. 18 Mezzi di chiarificazione

¹ Secondo le circostanze, le chiarificazioni comprendono segnatamente:

- a. informazioni raccolte per scritto o oralmente presso la controparte o l'avente economicamente diritto;
- b. visite nei luoghi in cui la controparte e l'avente economicamente diritto svolgono la loro attività;
- c. la consultazione delle fonti e delle banche dati pubblicamente accessibili;
- d. in caso di necessità, informazioni presso persone degne di fiducia.

² Le chiarificazioni sono effettuate nel rispetto della sfera privata delle persone interessate.

³ L'intermediario finanziario verifica la plausibilità dei risultati delle chiarificazioni e li documenta.

Art. 19 Delega delle chiarificazioni complementari a terzi

¹ Mediante accordo scritto, l'intermediario finanziario può dare mandato a persone e società di effettuare le chiarificazioni complementari se egli:

- a. si assicura che i mandatari eseguono le chiarificazioni con la stessa diligenza che egli stesso applicherebbe;
- b. istruisce i mandatari sui loro compiti;
- c. può controllare l'esecuzione diligente delle chiarificazioni effettuate dai mandatari.

² La subdelegazione da parte del mandatario è esclusa.

³ La documentazione relativa alle chiarificazioni deve essere depositata presso l'intermediario finanziario.

⁴ L'intermediario finanziario verifica la plausibilità dei risultati delle chiarificazioni.

Art. 20 Momento delle chiarificazioni complementari

Non appena i rischi superiori di una relazione d'affari diventano visibili, l'intermediario finanziario intraprende le chiarificazioni complementari e le porta a termine al più presto.

Art. 21 Ammissione di relazioni d'affari che presentano rischi superiori

L'ammissione di relazioni d'affari che presentano rischi superiori necessita l'accordo di una persona o di un organo superiore.

Art. 22 Responsabilità della direzione generale

¹ La direzione generale o almeno uno dei suoi membri prende le decisioni riguardanti:

- a. l'ammissione e, annualmente, il proseguimento delle relazioni d'affari con le persone politicamente esposte;
- b. l'applicazione, la sorveglianza e la valutazione dei controlli regolari di tutte le relazioni d'affari che comportano rischi superiori.

² Gli intermediari finanziari con un'attività di gestione patrimoniale molto importante e strutture con numerosi livelli gerarchici possono delegare questa responsabilità alla direzione di un'unità d'affari.

Sezione 6: Obblighi di documentazione

Art. 23 Disponibilità dell'informazione

L'intermediario finanziario organizza la propria documentazione in modo da essere in grado di fornire alle autorità penali o ad altre autorità autorizzate, entro un congruo termine, le informazioni e i documenti necessari a stabilire se un'impresa o una persona:

- a. è controparte o avente economicamente diritto;
- b. ha eseguito un'operazione di cassa che esige l'identificazione delle persone coinvolte;
- c. è al beneficio di una procura duratura su un conto o un deposito, nella misura in cui questa non risulti già da un registro ufficiale.

Sezione 7: Comportamento da osservare in caso di sospetto di riciclaggio di denaro o di relazioni con organizzazioni terroristiche

Art. 24 Comunicazione al momento dell'apertura delle relazioni d'affari

Se l'intermediario finanziario interrompe le trattative per l'apertura di una relazione d'affari a causa di un sospetto fondato di riciclaggio di denaro oppure di un legame con un'organizzazione terroristica o con un'organizzazione criminale di un altro tipo, lo comunica senza indugio all'Ufficio di comunicazione in materia di riciclaggio di denaro.

Art. 25 Relazioni con un'organizzazione terroristica

Se la chiarificazione del retroscena economico di transazioni inusuali rivela una relazione con un'organizzazione terroristica, l'intermediario finanziario lo comunica senza indugio all'Ufficio di comunicazione in materia di riciclaggio di denaro.

Art. 26 Comportamento in assenza di una decisione delle autorità

Se, entro il termine legale di cinque giorni feriali bancari dopo una comunicazione, l'intermediario finanziario non riceve dalle autorità di perseguimento penale una decisione che conferma il blocco dei beni, egli può decidere liberamente se e in quale misura mantenere la relazione d'affari.

Art. 27 Relazioni d'affari dubbiose e diritto di comunicazione

¹ Se un intermediario finanziario non ha sospetti fondati di riciclaggio di denaro ma le sue osservazioni gli permettono di concludere che determinati valori patrimoniali provengono da un crimine, egli può fare uso del diritto di comunicazione di cui all'articolo 305^{ter} capoverso 2 del Codice penale³ e comunicare le sue osservazioni alle autorità di perseguimento penale e all'Ufficio di comunicazione in materia di riciclaggio di denaro.

² L'intermediario finanziario esamina l'esercizio del suo diritto di comunicazione segnatamente per le relazioni d'affari che concernono importanti valori patrimoniali e documenta il risultato di tale esame.

Art. 28 Interruzione delle relazioni d'affari dubbiose

¹ Se l'intermediario finanziario pone termine a una relazione d'affari dubbiosa senza effettuare una comunicazione per mancanza di un sospetto fondato di riciclaggio di denaro, egli può autorizzare il prelievo di importanti valori patrimoniali unicamente in una maniera che, se necessario, permette alle autorità di perseguimento penale di seguirne la traccia («paper trail»).

² L'intermediario finanziario non può interrompere una relazione d'affari dubbiosa o autorizzare il prelievo di importanti valori patrimoniali se vi sono segni concreti di imminenti misure di sicurezza da parte di un'autorità.

Art. 29 Mantenimento delle relazioni d'affari dubbiose

L'intermediario finanziario che decide di mantenere una relazione d'affari dubbiosa deve sorvegliarla in modo particolare ed esaminarla sotto il profilo degli indizi di riciclaggio di denaro (Allegato).

Art. 30 Informazione della Commissione federale delle banche

L'intermediario finanziario informa la Commissione federale delle banche delle comunicazioni effettuate all'Ufficio di comunicazione in materia di riciclaggio di denaro riguardanti relazioni d'affari che con-

³ RS 311.0

cernono importanti valori patrimoniali o quando risulta verosimile, considerate le circostanze, che la vicenda che ha portato alla comunicazione si ripercuoterà sulla reputazione dell'intermediario finanziario o su quella della piazza finanziaria.

Sezione 8: Revisione

Art. 31

I revisori esterni degli intermediari finanziari, nonché quelli delle società del gruppo assoggettate alla sorveglianza della Commissione federale delle banche conformemente all'articolo 2 capoverso 2, controllano il rispetto delle disposizioni della presente ordinanza e prendono posizione in merito nel loro rapporto di revisione.

Sezione 9: Disposizioni finali

Art. 32 Disposizioni transitorie

¹ Gli intermediari finanziari devono conformarsi alle esigenze di cui agli articoli 3, 6-13, 15 e 17-22 entro il 30 giugno 2004. La Commissione federale delle banche può prorogare questo termine su richiesta motivata.

² Gli intermediari finanziari devono determinare le relazioni d'affari che presentano rischi superiori e designarle ad uso interno entro il 30 giugno 2004. A tale scopo possono di regola basarsi sui dati attuali e rinunciare a un'analisi retroattiva delle transazioni.

³ I sistemi di sorveglianza delle transazioni di cui all'articolo 12 devono rilevare le transazioni effettuate dopo il 30 giugno 2004.

⁴ Gli intermediari finanziari fanno esaminare i provvedimenti e lo scadenziario per l'applicazione della presente ordinanza dai loro revisori esterni e presentano in merito un rapporto alla Commissione federale delle banche entro il 30 settembre 2003.

⁵ Nei rapporti di revisione per l'esercizio 2004, i revisori esterni devono:

- a. presentare le misure con cui la presente ordinanza è stata applicata dagli intermediari finanziari;

b. indicare se tramite queste misure gli intermediari finanziari rispettano le esigenze della presente ordinanza.

⁶ Le società del gruppo che, al momento dell'entrata in vigore della presente ordinanza, esercitano un'attività di cui all'articolo 2 capoverso 3 LRD e che desiderano essere assoggettate alla sorveglianza della Commissione federale delle banche conformemente all'articolo 2 capoverso 2 della presente ordinanza o lo sono già in applicazione della Circolare 98/1 della Commissione federale delle banche devono inoltrare una richiesta motivata presso la Commissione federale delle banche entro il 30 settembre 2003. Le richieste possono essere inoltrate dal gruppo finanziario in modo centralizzato.

Art. 33 Entrata in vigore

La presente ordinanza entra in vigore il 1° luglio 2003.

18 dicembre 2002

In nome della Commissione federale
delle banche:

Il Presidente, Kurt Hauri

Il Direttore, Daniel Zuberbühler

Indizi di riciclaggio di denaro

I. Importanza degli indizi

A1 Gli indizi di riciclaggio indicati qui di seguito servono in primo luogo a sensibilizzare gli intermediari finanziari. Essi permettono di segnalare le relazioni d'affari o le transazioni che comportano un rischio superiore. Di regola la presenza di un singolo indizio non permette di fondare un sospetto sufficiente dell'esistenza di una transazione di riciclaggio. Il concorso di diversi di questi elementi può tuttavia indicarne la presenza.

A2 La plausibilità delle dichiarazioni dei clienti sul retroscena economico di tali operazioni deve essere esaminata. A questo riguardo è importante che non tutte le dichiarazioni del cliente (ad es. un rimando a motivi fiscali o alla legislazione sulle divise) siano accettate senza esame.

II. Indizi generali

Una transazione presenta rischi particolari di riciclaggio:

A3 quando la sua costruzione indica uno scopo illecito, il suo scopo economico non è riconoscibile oppure quando essa appare economicamente assurda;

A4 quando i valori patrimoniali sono ritirati poco tempo dopo essere stati versati (conto di passaggio), se l'attività commerciale del cliente non rende plausibile un tale ritiro immediato;

A5 quando non sono chiari i motivi per cui il cliente ha scelto proprio questo intermediario finanziario o questa sede per i suoi affari;

A6 quando essa ha per conseguenza che un conto, rimasto fino ad allora ampiamente inattivo, diventi molto attivo senza che se ne possa riscontrare un motivo plausibile;

A7 quando essa non è compatibile con le informazioni e le esperienze dell'intermediario finanziario concernenti il cliente o lo scopo della relazione d'affari.

A8 Deve inoltre essere considerato sospetto ogni cliente che comunica all'intermediario finanziario informazioni false o ingannevoli oppure che, senza ragioni plausibili, rifiuta di fornire i documenti o le informazioni usuali e necessarie per la relazione d'affari e per l'attività indicata.

A8^{bis} Può costituire un motivo di sospetto il fatto che un cliente riceva periodicamente bonifici da una banca con sede in uno dei Paesi considerati non cooperativi dal «Gruppo d'Azione Finanziaria (GAFI)», o che un cliente proceda in maniera ripetuta a bonifici in direzione di uno di questi Paesi.

III. Indizi specifici

1. Operazioni di cassa

A9 Cambio di un grosso importo in biglietti di banca di piccolo taglio (svizzeri o esteri) in biglietti di grosso taglio.

A10 Operazioni di cambio importanti, senza contabilizzazione sul conto di un cliente.

A11 Incasso di importi importanti tramite chèques, inclusi traveller's chèques.

A12 Acquisto o vendita di grandi quantità di metalli preziosi da clienti occasionali.

A13 Acquisto di chèques bancari per grossi importi da clienti occasionali.

A14 Ordini di bonifico all'estero dati da clienti occasionali, senza ragioni legittime apparenti.

A15 Frequente conclusione di operazioni di cassa fino a un importo di poco inferiore al limite al di sopra del quale è richiesta l'identificazione del cliente.

A16 Acquisto di titoli al portatore mediante consegna fisica.

2. Operazioni tramite conto o tramite depositi

A17 Ritiro frequente di grossi importi in contanti senza che l'attività del cliente giustifichi una tale operazione.

A18 Ricorso a metodi di finanziamento il cui impiego, per quanto usuale nel commercio internazionale, risulta contrario all'attività conosciuta del cliente.

A19 Conti utilizzati in maniera intensiva, quando normalmente questi conti non sono utilizzati o lo sono in modo assai minore.

A20 Struttura economica assurda della relazione d'affari tra il cliente e la banca (grande numero di conti presso lo stesso istituto, frequenti trasferimenti tra conti diversi, liquidità eccessiva, ecc.).

A21 Fornitura di garanzie (pegni, fidejussioni) da parte di terzi sconosciuti alla banca che non appaiono essere in stretta relazione con il cliente né avere un motivo plausibile e riconoscibile di fornire tali garanzie.

A22 Bonifici a favore di un'altra banca senza indicazione del beneficiario.

A23 Accettazione di bonifici da parte di altre banche senza indicazione del nome o del numero di conto del beneficiario o dell'ordinante.

A24 Bonifici ripetuti di somme importanti all'estero con ordine di pagamento in contanti al beneficiario.

A25 Bonifici importanti e ripetuti in direzione di o provenienti da Paesi produttori di droga.

A26 Fornitura di fidejussioni o di garanzie bancarie a titolo di garanzia per prestiti tra terzi non conformi alle condizioni del mercato.

A27 Versamenti in contanti da parte di un gran numero di persone diverse sul medesimo conto.

A28 Rimborso inatteso e senza spiegazioni convincenti di un credito compromesso.

A29 Uso di conti pseudonimi o numerici nell'esecuzione di transazioni commerciali da parte di imprese artigianali, commerciali o industriali.

A30 Prelievo di valori patrimoniali poco tempo dopo il loro accreditamento sul conto (conto di passaggio).

3. Operazioni fiduciarie

A31 Crediti fiduciari (back-to-back loans) senza scopo lecito riconoscibile.

A32 Detenzione fiduciaria di partecipazioni di società non quotate in borsa e la cui attività non può essere determinata dalla banca.

4. Altro

A33 Tentativi del cliente di sottrarsi al contatto personale con l'intermediario finanziario.

IV. Indizi qualificati

A34 Richiesta del cliente di chiudere un conto e di aprirne altri in nome proprio o in nome di membri della sua famiglia senza lasciare tracce nella documentazione della banca («paper trail»).

A35 Richiesta del cliente di ottenere ricevute per prelievi in contanti o per consegne di titoli che non si sono realmente verificati o che sono stati immediatamente depositati nello stesso istituto.

A36 Richiesta del cliente di effettuare ordini di bonifico con indicazione inesatta dell'ordinante.

A37 Richiesta del cliente di effettuare un bonifico non direttamente dal proprio conto ma da un conto «Nostro» dell'intermediario finanziario o da un conto «Diversi».

A38 Richiesta del cliente di accettare o fare documentare garanzie che non corrispondono alla realtà economica o di concedere crediti a titolo fiduciario in base a una copertura fittizia.

A39 Procedimenti penali contro il cliente dell'intermediario finanziario per crimini, corruzione o sottrazione di fondi pubblici.

The following is an unofficial translation. There is no official English version of Federal and SFBC legal texts. The legally binding version of this Ordinance will be available in German, French and Italian in the Official Collection of Federal Laws.

Ordinance of the Swiss Federal Banking Commission Concerning the Prevention of Money Laundering (SFBC Money Laundering Ordinance, MLO SFBC)

dated 18 December 2002

The Federal Banking Commission hereby issues the following Ordinance based on Article 16 (1) and Article 41 of the Swiss Money Laundering Act of 10 October 1997¹.

1. General provisions

Art. 1 Definitions

In this Ordinance the following terms shall have the following meanings:

- a. Politically exposed persons:
 1. the following persons holding prominent public positions abroad: heads of state or of government, senior politicians on the national level, senior government, judicial, military or party officials on the national level, or senior executives of state-owned enterprises of national importance;
 2. individuals or undertakings identified as having close family ties or personal or business connections to the aforementioned persons.
- b. Professional banknote dealers: non-banking institutions (individuals or undertakings) either within or outside Switzerland, which are engaged in buying and selling banknotes and earn significant income or revenues from such activity.

¹ SR 955.0

- c. Terrorist organizations: criminal organizations as defined under Article 260^{ter} of the Swiss Penal Code².
- d. Group companies: companies that pursuant to Capital Adequacy Regulations are included in the consolidated financial statements of a financial intermediary, as defined in Article 2 (1).

Art. 2 Scope

¹ This Ordinance applies to financial intermediaries as defined in Article 2 (2) (a), (b) and (d) of the Swiss Money Laundering Act ("Money Laundering Act")³, except for fund managers where responsibility for discharging the duties laid down in this Ordinance and the Money Laundering Act⁴ lies with the custodian bank.

² The Banking Commission may monitor any Swiss group company of a financial intermediary as defined in subparagraph 1, at its request, with respect to its compliance with the duties laid down in this Ordinance, provided that:

- a. it carries on a financial activity as defined under Article 2 (3) of the Money Laundering Act;
- b. it satisfies the conditions set out in Article 14 (2) of the Money Laundering Act;
- c. it acknowledges the Banking Commission's ability to take action against it, pursuant to Articles 19 and 20 of the Money Laundering Act;
- d. the Group undertakes to monitor compliance with the rules laid down in this Ordinance and to take action to enforce such rules;
- e. the Group undertakes to ensure that its external auditors verify compliance with this Ordinance and that they give an opinion in the Group auditor's report on each individual group company audited.

³ The Banking Commission publishes a list of group companies placed under its regulatory control in accordance with subparagraph 2 above.

² SR 311.0

³ SR 955.0

⁴ SR 955.0

Art. 3 Branch offices and group companies abroad

¹ Financial intermediaries shall ensure that their branch offices or group companies abroad, which operate in the financial sector, comply with the basic principles laid down in this Ordinance.

² They are obliged to inform the Banking Commission where:

- a. local regulations prevent compliance with the basic principles laid down in this Ordinance; or
- b. they would suffer a serious competitive disadvantage as a result.

³ The reporting of suspicious transactions or business relationships as well as any freeze on assets shall be governed by the rules and regulations of the host country.

2. Basic principles

Art. 4 Bar on accepting the proceeds of corruption or other crimes

¹ Financial intermediaries are not permitted to accept assets that, they know, or are expected to know, are the proceeds of criminal activities, even if committed outside Switzerland.

² The proceeds of criminal activities include in particular any assets obtained through corruption, embezzlement of public funds, abuse of an official function, or dishonest dealings by a public officer.

³ The negligent acceptance of assets derived from criminal activity may cause financial intermediaries to no longer meet the fit and proper requirement.

Art. 5 Bar on business relationships with criminal and terrorist organizations

Financial intermediaries are not permitted to maintain business relationships with any individuals or undertakings which, they know, or are expected to know, constitute a terrorist or criminal organization, or which are affiliated to, or support or finance such an organization.

Art. 6 Relationships with correspondent banks

¹ The provisions of this Ordinance also apply to correspondent banking relationships.

² Financial intermediaries shall not maintain any business relationship with banks that do not maintain a physical presence in the country under the laws of which they were established, unless they are part of a financial group subject to effective consolidated supervision.

3. Organizational measures

Art. 7 Higher risk business relationships

¹ Financial intermediaries shall formulate criteria to identify business relationships which involve higher legal or reputational risks.

² Depending on the type of operations conducted by the financial intermediary, the following criteria may be of particular relevance:

- a. the registered office, permanent place of residence, or nationality of the contracting partner and beneficial owner;
- b. the nature and location of the business activities conducted by the contracting partner and beneficial owner;
- c. the absence of personal contact with the contracting partner and beneficial owner;
- d. the type of services or products requested;
- e. the importance of the assets deposited;
- f. the importance of incoming and outgoing funds;
- g. the countries from which or to which frequent payments are made.

³ Business relationships with politically exposed persons shall always be deemed to involve higher risk.

⁴ Financial intermediaries shall identify any business relationships involving higher risk in accordance with subparagraphs 2 and 3 and label them as such for internal use.

Art. 8 Higher risk transactions

¹ Financial intermediaries shall formulate criteria for detecting transactions which involve increased legal or reputational risks.

² Depending on the type of operations conducted by the financial intermediary, the following criteria may be of particular relevance:

- a. the importance of incoming and outgoing assets;
- b. any significant divergence from the type, volume or frequency of transactions that would be normal in the context of the business relationship;
- c. any significant divergence from the type, volume or frequency of transactions that would be normal in comparable business relationships;

³ The following transactions shall always be deemed to involve higher risks,

- a. the physical deposit of assets exceeding CHF 100,000 in value, at the commencement of a business relationship, either involving a single or a series of deposits;
- b. transactions for which Indicators of Money Laundering are present (Schedule).

Art. 9 Global management of legal and reputational risks

¹ Financial intermediaries which have branch offices located outside Switzerland, or which control a financial group with non-Swiss group companies, are required to identify, mitigate and monitor the legal and reputational risks associated with money laundering or the financing of terrorism, on a global basis.

² Such financial intermediaries shall ensure that:

- a. the group's internal control bodies and external auditors are able to access information concerning specific business relationships in all group companies if needed. The creation of a centralized database of contracting partners and beneficial owners or a centralized access to local databases is not required;
- b. group companies supply to the Group's competent bodies the information necessary for the global management of legal and reputational risks.

³ If any financial intermediary notices that there is a bar or serious impediment to accessing information on contracting partners and bene-

ficial owners in certain countries, on legal or practical grounds, it shall inform the Banking Commission without delay.

⁴ Financial intermediaries forming part of a financial group, either from Switzerland or abroad, shall allow the Group's internal control bodies and external auditors to access any information which may be required concerning specific business relationships, provided that such information is essential for the management of legal and reputational risks on a global basis.

Art. 10 Internal anti-money laundering directives

¹ Financial intermediaries shall adopt internal directives concerning the prevention of money laundering and communicate them to all client advisors and any other relevant staff.

² Such directives shall set out:

- a. the criteria to be applied in identifying business relationships which involve higher risk as defined in Article 7;
- b. the criteria which must be applied in detecting transactions which involve higher risk as defined in Article 8 (1) and (2);
- c. the procedures for identifying, mitigating and monitoring such increased risks;
- d. the basic principles of the transaction monitoring system described in Article 12;
- e. the situations in which the internal anti-money laundering body must be consulted and the senior executive body notified;
- f. the basic principles of staff training;
- g. the corporate policy on politically exposed persons;
- h. the responsibility to file reports to the Money Laundering Reporting Office;
- i. the threshold amounts referred to in Article 7 (2) (e) and (f) and Article 8 (2) (a).

³ Directives shall be adopted by the board of directors or senior executive body.

Art. 11 Staff training

Financial intermediaries shall be responsible for providing regular training to client advisors and any other relevant staff on aspects of money laundering prevention which are of relevance to them.

Art. 12 Transaction monitoring system

¹ Financial intermediaries shall be responsible for setting up effective procedures for monitoring transactions and shall operate computer systems to facilitate the detection of higher risk transactions, as defined in Article 8 (1), (2) and (3) (a).

² Transactions identified by such a monitoring system must be analysed within a reasonable period of time. If necessary, additional investigations shall be carried out in accordance with Article 17.

³ Financial intermediaries with few contracting partners, beneficial owners or transactions may forgo the use of a computerized monitoring system, provided that their external auditors are instructed to carry out an in-depth special annual assessment of the monitoring of transaction.

Art. 13 Internal anti-money laundering body

¹ Financial intermediaries shall appoint one or more qualified individuals as part of their anti-money laundering bodies. Such bodies shall advise and assist line managers and the senior executive body in implementing this Ordinance without relieving them from their respective responsibilities.

² The internal anti-money laundering body is responsible for

- a. preparing internal anti-money laundering directives;
- b. monitoring the implementation of internal anti-money laundering directives in line with internal and external auditors and line management;
- c. planning and overseeing internal anti-money laundering training;
- d. defining the parameters for the transaction monitoring system described in Article 12;

- e. initiating the analysis of information generated by the transaction monitoring system;
- f. initiating additional investigations in accordance with Article 17, or conducting its own investigations;
- g. ensuring that the executive body responsible for making decisions regarding the commencement or continuation of business relationships in accordance with Article 22 (1) is supplied with any information necessary to take such decisions.

³ Financial intermediaries, while remaining liable, may also appoint external experts to execute the tasks of the internal anti-money laundering body, where:

- a. they are not in a position to appoint their own body due to their size or organizational structure; or
- b. the creation of such a body would be inappropriate.

4. General due diligence obligations

Art. 14 Verifying the identity of contracting partners and establishing the identity of beneficial owners

¹ All financial intermediaries are bound to comply with the provisions dealing with the verification of the identity of the contracting partner and identification of the beneficial owner laid down in the "Agreement on the Swiss Banks' Code of Conduct With Regard to the Exercise of Due Diligence" of 2 December 2002 (CDB 2003) made between the Swiss Bankers Association and the banks.

² Any breach of CDB 2003 may cause financial intermediaries to no longer meet the fit and proper requirement.

Art. 15 Originator information on wire-transfers

¹ In case of cross-border wire-transfers, financial intermediaries are required to include the name, account number and domicile, or the name and an identification number.

² Financial intermediaries may forgo to indicate such information for

legitimate reasons, for example in the case of recurring payments. Such reasons must be investigated and documented.

Art. 16 Professional banknote dealing

¹ Professional banknote trading may only be undertaken with banknote dealers which satisfy the requirements of a trustworthy correspondent bank relationship.

² Prior to commencing any business relationship, financial intermediaries are required to make enquiries into the nature of the business conducted by the banknote dealer and seek a commercial information and references.

³ Financial intermediaries shall set revenues and credit limits for their professional banknote dealing activities globally and for each counterparty. Financial intermediaries shall review the limits set at least once a year and monitor compliance to such limits on an ongoing basis.

⁴ Financial intermediaries which engage in professional banknote dealing shall issue directives in relation thereto, which must in principle be adopted by the senior executive body.

5. Enhanced due diligence obligations

Art. 17 Additional investigations in case of higher risk

¹ Financial intermediaries shall take measures proportional to circumstances to carry out additional investigations into business relationships or transactions involving higher risk.

² Depending on the circumstances, certain enquiries must be made, among others:

- a. whether the contracting partner is the beneficial owner of the assets deposited;
- b. the origin of the assets deposited;
- c. the purpose of withdrawals of assets;
- d. the rationale for large deposits;
- e. the provenance of the assets of the contracting partner and beneficial owner;

- f. the occupation or business activity of the contracting partner and beneficial owner;
- g. whether the contracting partner or beneficial owner is a politically exposed person;
- h. in the case of legal entities: who controls such entities.

Art. 18 Means of investigation

¹ Depending on the circumstances, investigations shall include, among others:

- a. obtaining information in written or oral form from the contracting partner or beneficial owner;
- b. visits of the places of business of contracting partner and beneficial owner;
- c. consultation of publicly accessible sources and databases;
- d. information from trustworthy individuals, where necessary.

² Any investigations shall respect the privacy of the individual concerned.

³ Financial intermediaries shall review the results of the investigations carried out with a view to their plausibility and keep records of such investigations and their results.

Art. 19 Delegation of additional investigations to third parties

¹ Financial intermediaries may appoint individuals or undertaking to carry out additional investigations under written agreement, provided that the financial intermediary concerned

- a. ensures that such party exercises the same due diligence in carrying out its investigations as would be exercised by the financial intermediary itself;
- b. issues specific instructions to such party regarding the duties delegated;
- c. is in a position to verify that such investigations are carried out with due diligence.

² The party appointed shall not be permitted to further delegate the concerned duties.

³ Records relating to investigations carried out must be left with the financial intermediary.

⁴ Financial intermediaries shall review the results of the investigations carried out with a view to their plausibility.

Art. 20 Timing of additional investigations

As soon as it becomes evident that a business relationship entails higher risk, financial intermediaries shall initiate the additional investigations required and complete such investigations as quickly as possible.

Art. 21 Commencement of business relationships involving higher risks

No business relationship which involves increased risk may be commenced without the approval of a person or body of a superior level of authority.

Art. 22 Responsibilities of the most senior executive body

¹ The most senior executive body, or at least one of its members, shall be responsible for making decisions:

- a. regarding the commencement, and on an annual basis the continuation of business relationships with politically exposed persons;
- b. on initiating regular reviews of all business relationships involving higher risk and monitoring and evaluating such relationships.

² Financial intermediaries engaged in extensive asset management operations and with multilevel hierarchical structures may assign such responsibilities to the management of a business unit.

6. Record-keeping requirements

Art. 23 Availability of information

Financial intermediaries are required to set up a record-keeping system which would enable them to inform and supply the relevant documents to the prosecuting authorities, or any other competent authority, within a reasonable period of time and to provide information on undertakings or individuals who:

- a. are the contracting partners or beneficial owners;
- b. have carried out a cash transaction necessitating identification of the person concerned;
- c. have a permanent power of attorney over an account or custody account, unless such power of attorney is recorded in a public register.

7. Course of action in case of indications of money laundering activity or connections to terrorist organizations

Art. 24 Filing a report at commencement of the business relationship

If a financial intermediary terminates negotiations aimed at concluding business relationship because of substantiated reasonable grounds to suspect money laundering activity or links with a terrorist or other criminal organization, it shall report the matter to the Money Laundering Reporting Office promptly.

Art. 25 Links with terrorist organizations

Where the investigation of the background of an unusual transaction reveals links to a terrorist organization, the financial intermediary shall report the matter to the Money Laundering Reporting Office promptly.

Art. 26 Course of action to be taken in the absence of any decision by the authorities

If the financial intermediary has not received any official order authorizing it to continue freezing the assets, within the statutory limit of five working days after filing a report with the prosecuting authorities, it may decide at its discretion whether, or under what conditions, it wishes to continue the business relationship.

Art. 27 Dubious business relationships and the right to file a report

¹ Financial intermediaries which have no clear evidence for suspecting money laundering activity, but have information suggesting that assets

are derived from criminal activities, are entitled to file a report with the prosecuting authorities and the Money Laundering Reporting Office, based on the reporting right conferred by Article 305^{ter} (2) of the Swiss Penal Code⁵.

² In case of business relationships involving significant assets, financial intermediaries shall specifically assess whether to exercise their right to report and document the outcome of such assessment.

Art. 28 Terminating dubious business relationships

¹ If a financial intermediary terminates a dubious business relationship without filing a report because of the absence of specific evidence justifying suspicion of money laundering activity, it may only permit withdrawal of large amounts of assets in a form which would allow the prosecuting authorities to track such funds by means of a paper trail.

² Financial intermediaries may not terminate a dubious business relationship, or permit the withdrawal of substantial amounts of assets, if there are concrete indications that action by the authorities to impound the assets is imminent.

Art. 29 Continuation of dubious business relationships

Where a financial intermediary decides to continue a dubious business relationship, it shall monitor such relationship carefully and assess whether any indicators of money laundering are present (Schedule).

Art. 30 Informing the Banking Commission

Financial intermediaries shall inform the Banking Commission of any business relationship involving significant assets, which have been reported to the Money Laundering Reporting Office, or if, given the circumstances, there are reasons to believe that the events giving rise to such report could affect the reputation of the financial intermediary and that of the financial center.

⁵ SR 311.0

8. Audit review

Art. 31 Review by external auditors

The external auditors of the financial intermediary or the group company subject to the supervision of the Banking Commission in accordance with Article 2 (2), shall monitor the compliance with the provisions of this Ordinance and give opinions regarding such matter in the auditors report.

9. Final provisions

Art. 32 Transitional provisions

¹ Financial intermediaries shall satisfy the requirements stipulated in Articles 3, 6 to 13, 15 and 17 to 22 of this Ordinance by 30 June 2004. The Banking Commission may extend this period upon request and provided that legitimate reasons are shown.

² Financial intermediaries are required to identify internally all existing business relationships presenting higher risks by 30 June 2004. As a general principle, financial intermediaries may rely on current data and are not required to analyse transactions retrospectively.

³ The transaction monitoring systems described in Article 12 of this Ordinance must cover transactions carried out after 30 June 2004.

⁴ Financial intermediaries are required to submit an action plan and timetable to their external auditors for review and report to the Banking Commission by 30 September 2003.

⁵ In their auditor's report for the financial year 2004, external auditors shall

- a. describe the ways in which financial intermediaries have implemented this Ordinance;
- b. comment on whether such measures satisfy the requirements of this Ordinance.

⁶ Group companies which are carrying on a business, as defined in Article 2 (3) of the Swiss Money Laundering Act⁶, on the date on which this Ordinance takes effect, and wish to be regulated by the Banking Commission pursuant to Article 2 (2) of this Ordinance, or are already

⁶ SR 955.0

subject to its control by reason of Banking Commission Circular 98/1, shall file a motivated request with the Banking Commission by 30 September 2003. Applications may be made centrally by the financial group.

Art. 33 Entry into force

This Ordinance takes effect on 1 July 2003.

Schedule: Indicators of Money Laundering

For and on behalf of the Swiss Federal
Banking Commission

Chairman: Kurt Hauri
Director: Daniel Zuberbühler

Indicators of Money Laundering

I. Significance of indicators

A1 The indicators for potential money laundering activity set out below are primarily intended to raise awareness among the staff of financial intermediaries. These indicators enable identification and the reporting of higher risk business relationships or transactions. A single indicator may not in itself be sufficient grounds for suspecting that a illegal money laundering transaction has been carried out, but the existence of more than one such factor may be indicative of money laundering activity.

A2 The plausibility of the client's explanations regarding the background to such transactions must be assessed. In this connection, it is important that explanations provided by the client (e.g. by citing tax or exchange regulations as reasons) are not necessarily accepted at face value.

II. General indicators

Particular money laundering risks are inherent in transactions

A3 where the structure indicates some illegal purpose, their commercial purpose is unclear or appears absurd from a commercial point of view;

A4 involving a withdrawal of assets shortly after funds have been deposited with the financial intermediary (pass-through accounts), provided that the instant withdrawal of such assets cannot be accounted for on the basis of the client's business activity;

A5 where the client's reason for selecting this particular financial intermediary or branch to carry out its transactions is unclear;

A6 resulting in significant, but unexplained, activity on an account which was previously mostly dormant;

A7 which are inconsistent with the financial intermediary's knowledge and experience of the client and the stated purpose of the business relationship.

A8 Clients who supply false or misleading information to financial intermediaries, or refuse for no credible reason to provide information and documents which are required and routinely supplied in relation to the relevant business activity, must be treated with suspicion.

A8^{bis} There may be grounds for suspicion if a client regularly receives transfers of funds from a bank domiciled in a country deemed to be uncooperative by the Financial Action Task Force (FATF), or makes repeated transfers to such a country.

III. Specific indicators

1. Over the counter transactions

A9 The exchange of a large amount of small-denomination banknotes (foreign and domestic) for large-denomination banknotes;

A10 The exchange of large amounts of money without crediting a client account;

A11 Cashing cheques for large sums, including travellers' cheques;

A12 The purchase or sale of large amounts of precious metals by occasional clients;

A13 The purchase of banker's drafts for large amounts by occasional clients;

A14 Instructions to make a transfer abroad by occasional clients, without apparent legitimate reason;

A15 The execution of multiple cash transactions just below the threshold for which client identification is required;

A16 The acquisition of bearer instruments by means of physical delivery.

2. Bank accounts and custody accounts

A17 Frequent withdrawals of large amounts of cash which cannot be explained by reason of the client's business;

A18 Use of loan facilities that, while normal in international trade, is inconsistent with the known activity of the client;

A19 Accounts through which a large number of transactions are routed, though such accounts are not normally used, or only used to a limited extent;

A20 The structure of the client's business relationships at the bank lacks a logical rationale (large number of accounts at the same bank, frequent transfers between accounts, excessive liquidity, etc.);

A21 Provision of security (pledges, guarantees) by third parties unknown to the bank, who have no obvious affiliation to the client and who have no credible and apparent reasons to provide such guarantees;

A22 Making transfers to another bank without supplying details of the beneficiary;

A23 Accepting funds transferred from other banks when the name or account number of the beneficiary or remitter has not been supplied;

A24 Repeated transfers of large amounts of money abroad with instructions that the sum be paid to the beneficiary in cash;

A25 Transfers of large amounts, or frequent transfers, to or from countries producing illegal drugs;

A26 Providing surety bonds or bank guarantees by way of security for third party loans, which have not been agreed on market terms;

A27 A large number of different individuals make cash deposits into a single account;

A28 Unexpected repayment of a non-performing loan without any credible explanation;

A29 Use of pseudonym or numbered accounts to carry out commercial transactions for trading, manufacturing or industrial concerns;

A30 Withdrawal of funds shortly after these have been credited to the account (pass-through account).

3. Fiduciary transactions

A31 Fiduciary loans (back-to-back loans) for which there is no obvious legal purpose;

A32 The holding of shares in unlisted companies in a fiduciary capacity, where the bank has no knowledge of the business conducted by such companies.

4. Other

A33 Client tries to evade attempts by the financial intermediary to establish personal contact.

IV. Indicators giving rise to particular suspicion

A34 Client requests accounts to be closed and to open new accounts in his own name, or in the name of a family member, without leaving a paper trail;

A35 Client requests receipts for cash withdrawals or deliveries of securities which in effect never took place, followed by the immediate deposit of such assets at the same bank;

A36 Client requests payment orders to be executed with incorrect remitter's details;

A37 Client requests that certain payment be routed through nostro accounts held by the financial intermediary or sundry accounts instead of its own account;

A38 Request by the client to accept or record in the accounts loan collateral which is inconsistent with commercial reality, or grant fiduciary loans for which notional collateral is recorded in the accounts.

A39 Client of financial intermediary has been prosecuted for a criminal offence, corruption or misuse of public funds.

EBK-Geldwäschereibericht

Bericht der Eidgenössischen Bankenkommission zu ihrer Geldwäschereiverordnung vom 18. Dezember 2002

März 2003

Vorwort

Dieser Bericht stützt sich wesentlich auf denjenigen der «Arbeitsgruppe KYC», der im Juli 2002 zusammen mit dem Vernehmlassungsentwurf der EBK-Geldwäschereiverordnung veröffentlicht wurde.¹ Er wurde aber aktualisiert und den seitherigen Entwicklungen und vor allem den Änderungen², welche die EBK aufgrund der Vernehmlassung vornahm, angepasst.

Die Erläuterungen in diesem Bericht können nicht alle Fragen im Detail beantworten, welche sich für die Banken bei der (anspruchsvollen) Umsetzung der neuen Regulierung stellen. Der Bericht soll einzig einzelne Zusammenhänge erläutern und in wichtigen Punkten aufzeigen, was eine Bestimmung beabsichtigt oder (was ebenso wichtig sein kann) nicht beabsichtigt. Unklarheiten werden im Übrigen im Dialog zwischen der EBK, den Banken und den Revisionsstellen zu klären sein. Die EBK möchte wenn immer möglich zusätzliche Mikroregulierungen zu Einzelpunkten vermeiden und höchstens dann regulierend eingreifen, wenn dies aus Gründen einer minimalen Einheitlichkeit in der Rechtsanwendung notwendig ist. Die Geldwäschereiverordnung verfolgt einen risikoorientierten Ansatz. Da die Risiken bei jedem Finanzintermediär unterschiedlich sind, werden es zwangsläufig auch

¹ «Sorgfaltspflichten von Banken und Effektenhändlern bei Geldwäscherei, Terrorismusfinanzierung und Beziehungen zu politisch exponierten Personen», Bericht einer durch die Eidg. Bankenkommission eingesetzten Arbeitsgruppe zum Entwurf einer Verordnung der Eidgenössischen Bankenkommission, Juni 2002, verfügbar auf der EBK-Website <http://www.ebk.admin.ch/d/archiv/2002/neu090702-02d.pdf>.

² Siehe Anhang I.

die Lösungen bei der Umsetzung der Verordnung sein. Die EBK denkt nicht, diesen Ansatz bei der Rechtsanwendung wieder ins Gegenteil zu verkehren.

Inhaltsverzeichnis

1	Übersicht	101
2	Revision der geltenden Regelung	105
2.1	Ausgangslage	105
2.2	Arbeitsgruppe KYC	106
2.3	Vernehmlassung	107
3	Nationale Rahmenbedingungen	110
3.1	Entwicklungen in der Gesetzgebung	111
3.2	Institutioneller Rahmen	113
3.3	Aufsichtsrecht und die Rolle der EBK	114
3.4	Selbstregulierung der Banken	115
4	Internationale Entwicklungen	116
4.1	Die 40 FATF-Empfehlungen (Juni 1996)	117
4.2	FATF-Empfehlungen gegen die Terrorismusfinanzierung	117
4.3	Terrorismusfinanzierungskonvention (Dezember 1999)	118
4.4	Wolfsberg-Prinzipien (2000/2002)	119
4.5	«Customer Due Diligence Paper» des Basler Ausschusses (Oktober 2001)	119
4.6	«Supervisors' PEP working paper 2001» (November 2001)	120
4.7	Weitere wichtige internationale Rechtsinstrumente	121
4.8	IWF – Financial Sector Assessment Switzerland (Juni 2002)	122
5	Grundzüge der Verordnung	123
5.1	Verordnung an Stelle der Geldwäschereirichtlinien	123
5.2	Inhaltliche Abgrenzung zur Selbstregulierung	124
5.3	Entwicklung der Regeln über politisch exponierte Personen	125
5.4	Risikoorientierte Sorgfalt bei erhöhten Risiken	126
5.5	Systematische Überwachung von Transaktionen	127
5.6	E-Banking	128
5.7	Globale Überwachung von Reputationsrisiken	129
5.8	Kampf gegen die Terrorismusfinanzierung	130
6	Sorgfaltspflichtvereinbarung	130
7	Kommentar zur Verordnung	133

7.1 Allgemeine Bestimmungen	133
7.2 Grundsätze	136
7.3 Organisatorische Massnahmen	138
7.4 Allgemeine Sorgfaltspflichten	146
7.5 Erhöhte Sorgfaltspflichten	148
7.6 Dokumentationspflichten	154
7.7 Verhalten bei Hinweisen auf Geldwäscherei oder Verbindungen mit terroristischen Organisationen	154
7.8 Revision	157
7.9 Schlussbestimmungen	157
Anhang I: Grundlegende Änderungen der Verordnung nach erfolgtem Vernehmlassungsverfahren	160

Abkürzungsverzeichnis

AFG, Anlagefondsgesetz	Bundesgesetz über die Anlagefonds vom 18. März 2000 (SR 951.31)
BankG, Bankengesetz	Bundesgesetz vom 8. November 1934 über die Banken und Sparkassen (SR 952.0)
Basler Ausschuss	Basler Ausschuss für Bankenaufsicht
BEHG, Börsengesetz	Bundesgesetz über die Börsen und den Effektenhandel vom 24. März 1995 (SR 954.1)
Botschaft	Botschaft des Bundesrates
CDD	Customer Due Diligence for Banks (Sorgfaltspflichten der Banken bei der Feststellung der Kundenidentität), Papier des Basler Ausschusses, Oktober 2001
EBK, Bankenkommission	Eidgenössische Bankenkommission
FATF	Financial Action Task Force
Geldwäschereirichtlinien	Richtlinien zur Bekämpfung und Verhinderung der Geldwäscherei vom 26. März 1998 (RS-EBK 98/1)
GwG, Geldwäschereigesetz	Bundesgesetz zur Bekämpfung der Geldwäscherei im Finanzsektor vom 10. Oktober 1997 (SR 955.0)
GwV-EBK, Verordnung	Verordnung der Eidgenössischen Bankenkommission zur Verhinderung der Geldwäscherei vom 18. Dezember 2002
IWF	Internationaler Währungsfonds
Kontrollstelle	Kontrollstelle für die Bekämpfung der Geldwäscherei
Meldestelle	Meldestelle für Geldwäscherei
neuStGB	Änderung des Schweizerischen Strafgesetzbuches und des Militärstrafgesetzes vom 14. Dezember 2002 (BBl 1999 1976; SR 311.0)
PEP	Politically Exposed Persons: Politisch exponierte Personen
SBVg	Schweizerische Bankiervereinigung
StGB	Schweizerisches Strafgesetzbuch vom 21. Dezember 1937 (SR 311.0)

Sorgfaltspflichtsverordnung	Verordnung der Kontrollstelle über die Sorgfalts-
der Kontrollstelle	pflichten der Finanzintermediäre (955.033.2)
Terrorismusfinanzierungs-	Internationales Übereinkommen zur Bekämpfung der
konvention	Finanzierung des Terrorismus vom 9. Dezember 1999
VSB, Sorgfaltspflicht-	Vereinbarung über die Standesregeln zur Sorgfalts-
vereinbarung	pflicht der Banken vom 28. Januar 1998

1 Übersicht

Die EBK überwacht als spezialgesetzliche Aufsichtsbehörde im Sinne des Geldwäschereigesetzes die Einhaltung der vom Geldwäschereigesetz vorgeschriebenen Pflichten bei den ihrer Aufsicht unterstellten Instituten. Artikel 41 des Geldwäschereigesetzes gibt der EBK die Kompetenz, Vollzugsbestimmungen zu erlassen.

Die EBK hatte im April 2001 eine Arbeitsgruppe beauftragt, eine Revision der geltenden Regelung in die Wege zu leiten. Diese legte im Juni 2002 einen Entwurf für eine auf das Geldwäschereigesetz gestützte Verordnung der EBK vor, welche die geltenden Geldwäschereirichtlinien der EBK ersetzen sollte.³ Die Verordnung wurde nach einem öffentlichen Vernehmlassungsverfahren am 18. Dezember 2002 von der EBK beschlossen und tritt am 1. Juli 2003 in Kraft.

Während die Verordnung ausführt, welche Sorgfaltspflichten bei Geschäftsbeziehungen mit erhöhten Risiken gelten (Art. 6 GwG), regelt die Sorgfaltspflichtvereinbarung der SBVg, welche ebenfalls revidiert wurde⁴, wie bisher die für alle Kundenbeziehungen geltenden Identifizierungsgrundsätze. Im Vergleich zur bestehenden Regelung beinhaltet die Verordnung folgende wesentliche Neuerungen:

- Finanzintermediäre sollen bei der Geldwäschereiprävention einen risikoorientierten Ansatz anwenden. Bei Geschäftsbeziehungen mit erhöhten Risiken werden zusätzliche Abklärungen verlangt, zum Beispiel über die Herkunft der Vermögenswerte. Dies bedingt, dass die Finanzintermediäre vorher entsprechend ihrer Geschäftsaktivitäten Risikokriterien bilden und gestützt darauf alle bestehenden und neuen Geschäftsbeziehungen mit erhöhten Risiken feststellen und intern kennzeichnen. Bei den übrigen Geschäftsbeziehungen, die keine erhöhten Risiken aufweisen, sind hingegen neben der üb-

³ Siehe Fussnote 1.

⁴ Sorgfaltspflichtvereinbarung der Banken (VSB) 2003, auf dem Internet verfügbar unter <http://www.swissbanking.org/vsb-03-140103-mit-formularen.pdf>.

lichen Identifizierung nach Massgabe der Sorgfaltspflichtvereinbarung keine zusätzlichen Abklärungen erforderlich.

- Die Verordnung nimmt die bereits heute bestehende Regelung zu Geschäftsbeziehungen mit politisch exponierten Personen auf. Der Entscheid, solche Geschäftsbeziehungen aufzunehmen, weiterzuführen oder abzubrechen, hat auf Stufe der obersten Geschäftsleitung zu erfolgen. Untersagt ist jede Annahme von Vermögenswerten, von denen der Finanzintermediär weiss oder annehmen muss, dass sie aus einem Verbrechen, sei es im In- oder Ausland, herrühren. Dieses Verbot gilt insbesondere auch für solche Vermögenswerte, die aus Korruption und dem Missbrauch öffentlicher Gelder stammen.
- Neu sollen die bisher nur zur Bekämpfung der Geldwäscherei eingesetzten Instrumente auch zur Bekämpfung der Terrorismusfinanzierung angewandt werden.⁵ Weist die Abklärung des Hintergrundes ungewöhnlicher oder verdächtiger Transaktionen auf eine Verbindung zu einer terroristischen Organisation hin, so hat der Finanzintermediär unverzüglich eine Meldung an die Meldestelle für Geldwäscherei zu erstatten.
- Bei Zweifeln über eine Geschäftsbeziehung haben die Finanzintermediäre zu prüfen, ob sie von ihrem Melderecht Gebrauch machen und die Zweifel der Meldestelle melden wollen. Dies gilt insbesondere für Geschäftsbeziehungen mit bedeutenden Vermögenswerten.
- Mit Ausnahme kleinerer Institute haben alle Banken und Effektenhändler informatikgestützte Systeme zur Transaktionsüberwachung einzusetzen. Diese Systeme sollen helfen, ungewöhnliche Transaktionen zu ermitteln. Letztere sind anschliessend binnen angemessener Frist auszuwerten. Wenn nötig sind zusätzliche Abklärungen zur Geschäftsbeziehung in die Wege zu leiten.
- In Umsetzung der von der Financial Action Task Force (FATF) entwickelten Standards zur Bekämpfung der Terrorismusfinanzierung sollen alle Zahlungsaufträge ins Ausland Angaben über die auftraggebende Vertragspartei enthalten.

⁵Vgl. Ziff. 5.8.

- Die Verordnung formalisiert das Regime der Geldwäschereirichtlinien und erfasst nunmehr ausdrücklich neben Banken und Effektenhändlern auch Gesellschaften, die einer Gruppe mit Banken- oder Effektenhändlerstatus angehören, ohne selbst über eine Banken- oder Effektenhändlerbewilligung zu verfügen. Diese Gesellschaften können sich auf ein formelles Gesuch hin hinsichtlich der Einhaltung der Pflichten der Verordnung der Aufsicht der EBK unterstellen. Gesuche für Gruppengesellschaften, die bei Inkrafttreten dieser Verordnung eine Tätigkeit nach Artikel 2 Absatz 3 des Geldwäschereigesetzes ausüben und sich der Geldwäschereiaufsicht durch die EBK unterstellen wollen, sind bis Ende September 2003 der EBK einzureichen. Die Gesuche können zentral durch die Finanzgruppe erfolgen.
- Die Verordnung verdeutlicht die Regelung des Rundschreibens, wonach es schweizerischen Finanzintermediären verboten ist, ihre ausländischen Zweigniederlassungen und Gruppengesellschaften zur Umgehung der schweizerischen Regelungen zu benutzen. Die Verordnung verlangt, dass die Finanzintermediäre dafür sorgen, dass ihre ausländischen Zweigniederlassungen und Gruppengesellschaften die grundlegenden Prinzipien der Verordnung befolgen. Entsprechen die Schweizer Regeln nicht lokalem Recht oder Gebräuchen, könnte Schweizer Bankgruppen dadurch ein Wettbewerbsnachteil entstehen. In diesem Fall muss die EBK im Einzelfall eine Lösung mit den zuständigen Aufsichtsbehörden und betroffenen Instituten finden.
- Finanzintermediäre mit Zweigniederlassungen und Gruppengesellschaften im Ausland müssen alle ihre Rechts- und Reputationsrisiken global erfassen, begrenzen und überwachen. Sie haben sicherzustellen, dass die zuständigen Organe der Gruppe die dafür wesentlichen Informationen von den ausländischen Zweigniederlassungen und Gruppengesellschaften erhalten. Die internen Überwachungsorgane und die externen Revisoren der Gruppe sollen im Bedarfsfall Zugang zu Informationen über einzelne Geschäftsbezie-

hungen in allen Zweigniederlassungen und Gruppengesellschaften haben können.

- Die Bestimmungen der Verordnung gelten auch für Korrespondenzbankenbeziehungen. Für Banken ohne physische Präsenz im Inkorporationsort («shell banks») dürfen keine Korrespondenzkonti geführt werden. Es sei denn, es handelt sich um Tochtergesellschaften einer angemessen konsolidiert überwachten Finanzgruppe.
- Die Verordnung integriert die Bestimmungen, die heute in den Richtlinien für die Reglementierung des professionellen Notenhandels in den Banken vom 6. April 1990⁶ enthalten sind.

Mit Inkrafttreten der Verordnung am 1. Juli 2003 werden die folgenden Erlasse der EBK aufgehoben:

- die Richtlinien der Bankenkommission vom 6. April 1990 für die Reglementierung des professionellen Notenhandels in den Banken;
- die Mindeststandards der Bankenkommission für reine Internet-Banken und -Effekthändler zur Kontoeröffnung auf dem Korrespondenzweg und zur Kontoüberwachung vom 29. März 2001. Die betroffenen Banken und Effekthändler haben diese Mindeststandards indes bis zu dem Zeitpunkt zu befolgen, ab welchem sie die Vorschriften der EBK-Geldwäschereiverordnung und der Sorgfaltspflichtvereinbarung 2003 anwenden werden.

Das Rundschreiben 98/1 der EBK vom 26. März 1998 (Richtlinien zur Bekämpfung und Verhinderung der Geldwäscherei) wird am 30. Juni 2004 aufgehoben. Bis zu diesem Zeitpunkt gehen die Vorschriften der Verordnung vor, für welche keine Übergangsfrist besteht.

Für die Umsetzung einzelner Bestimmungen gewährt die Verordnung eine Übergangsfrist von einem Jahr, d.h. bis Ende Juni 2004. Alle übrigen sich aus der Verordnung ergebenden Pflichten erlangen mit dem 1. Juli 2003 Verbindlichkeit. Die Finanzintermediäre haben bis Ende

⁶ EBK Bulletin 20, 1990, S. 101.

Juni 2004 namentlich alle bis zu diesem Zeitpunkt bereits bestehenden Geschäftsbeziehungen mit erhöhten Risiken zu ermitteln und intern zu kennzeichnen.

Die Verordnung verlangt von den Finanzintermediären, dass sie Ende September 2003 der EBK über den Stand der Umsetzung Bericht erstatten und ihr ein Konzept sowie einen Zeitplan mit einer Prüfungsbestätigung ihrer Revisionsstelle vorlegen. Die EBK wird im Frühjahr 2003 allen betroffenen Finanzintermediären einen Fragebogen zustellen, welcher zum Zweck der Berichterstattung zu verwenden ist. Die EBK beabsichtigt nicht, in diesem Rahmen die Umsetzungskonzepte und Transaktionsüberwachungssysteme im Einzelnen zu beurteilen und abzunehmen. Sie will sicherstellen, dass die Umsetzung der Verordnung auf gutem Weg ist, und wird nur bei grundsätzlichen Problemen intervenieren.

2 Revision der geltenden Regelung

2.1 Ausgangslage

Die EBK erliess ihre ersten Geldwäschereirichtlinien⁷ im Jahre 1991 nach der Inkraftsetzung der Bestimmungen des Strafgesetzbuches über die Geldwäscherei⁸ und die mangelnde Sorgfalt bei Finanzgeschäften.⁹ Diese Richtlinien wurden im Jahr 1998 total revidiert¹⁰, insbesondere um den Entwicklungen der internationalen Standards auf dem Gebiet der Geldwäscherei Rechnung zu tragen.¹¹

In den Jahren 2000 und 2001 erlangten die Fälle Abacha und Montesinos¹², in welche auch Schweizer Banken verwickelt waren, sowohl

⁷ EBK-RS 91/3.

⁸ Art. 305^{ter} StGB.

⁹ Art. 305^{ter} StGB.

¹⁰ EBK-RS 98/1.

¹¹ Siehe Aufzählung in Randziffer 2 EBK-RS 98/1.

¹² Vgl. die Medienorientierungen der EBK in den Fällen Abacha und Montesinos unter <http://www.ebk.admin.ch/d/archiv/2000/archiv2000.htm>; <http://www.ebk.admin.ch/d/archiv/2001/archiv2001.htm>.

auf nationaler als auch internationaler Ebene Publizität und gaben zu der Frage Anlass, ob eine weitere Verschärfung der geltenden Regelung erforderlich sei. Die EBK erachtete die bestehende Regelung grundsätzlich für zweckmässig, sah aber in einzelnen Punkten Anpassungsbedarf. Sie beschloss daher, eine Revision der geltenden Geldwäschereirichtlinien in die Wege zu leiten. Einen weiteren Anstoss dafür lieferte die Einführung neuer Strafbestimmungen zur Bestechung ausländischer Beamter, die im Mai 2000 in Kraft traten.¹³ Schliesslich sollte auch die Weiterentwicklung der internationalen Geldwäschereistandards im Rahmen der Revision Berücksichtigung finden.

2.2 Arbeitsgruppe KYC

Im April 2001 beauftragte die Bankenkommission eine Arbeitsgruppe («Arbeitsgruppe KYC») mit der Revision der Geldwäschereirichtlinien. Die Arbeitsgruppe mit Vertretern der Schweizerischen Bankiervereinigung, des Schweizer Verbandes unabhängiger Effekthändler, der Aufsichtskommission VSB, der Schweizerischen Treuhand-Kammer, der Swiss Association of Compliance Officers, der kantonalen Strafbehörden, der Kontrollstelle und der Meldestelle wurde von EBK-Vizedirektor Dr. Urs Zulauf geleitet.

Diese Arbeitsgruppe sollte dabei gemäss Beschluss der EBK namentlich überprüfen, inwieweit die weitgehend auf dem Grundsatz «one size fits all» beruhenden Geldwäschereirichtlinien durch eine differenziertere Regelung ersetzt werden und ob strengere Sorgfaltspflichten und spezielle Überwachungspflichten im Private Banking gelten sollten. Bestandteil des Mandats der Arbeitsgruppe waren unter anderem auch die Fragen, ob besondere Anforderungen bei «non face to face»-Beziehungen und im Bereich des E-Banking gelten sollten und unter welchen Voraussetzungen eine Delegation von Abklärungen möglich sein sollte. Im Juni 2002 legte die Arbeitsgruppe einen Ent-

¹³ Art. 322^{septies} StGB, in Kraft seit 1. Mai 2000.

wurf für eine auf das Geldwäschereigesetz gestützte Verordnung der EBK mit einem Begleitbericht vor.¹⁴

2.3 Vernehmlassung

Im Juli 2002 veröffentlichte die EBK den Entwurf der Arbeitsgruppe KYC zur Vernehmlassung und lud alle interessierten Kreise zur Stellungnahme ein. Der Entwurf der Arbeitsgruppe stiess in der Vernehmlassung weitgehend auf positive Resonanz. Die Vernehmlassungsteilnehmer begrüßten namentlich den nun ausdrücklich in der Verordnung verankerten risikoorientierten Ansatz bei der Geldwäscherei-prävention. Einzelne Vorschläge der Arbeitsgruppe gaben hingegen Anlass zu Kritik:

- Verschiedene Vernehmlassungsteilnehmer kritisierten die extraterritoriale Anwendung der Verordnung auf ausländische Zweigniederlassungen und Gruppengesellschaften. Die EBK entschied trotz dieser Bedenken die Bestimmung beizubehalten, wonach Schweizer Finanzintermediäre sicherzustellen haben, dass ihre ausländischen Zweigniederlassungen und Gruppengesellschaften «die grundlegenden Prinzipien» der Verordnung befolgen. Diese Bestimmung dient der Präzisierung des bereits im geltenden Rundschreiben vorhandenen Umgehungsverbots. Sie beruht auf dem Grundsatz, dass die Geldwäschereibekämpfung nur effektiv ist, wenn in den ausländischen Zweigniederlassungen und Gruppengesellschaften ein Abwehrdispositiv vorhanden ist, welches den schweizerischen Anforderungen genügt. Die EBK beabsichtigt, mit dieser Regelung einer Aufsichtsarbitrage vorzubeugen.
- Auf Kritik stiess auch die Pflicht zur globalen Überwachung der Rechts- und Reputationsrisiken innerhalb einer Finanzgruppe. Gegen den dazu erforderlichen konzernweiten Informationsaustausch wurde eingewandt, dass die aktuelle Rechtslage in zahlreichen Ländern den Datentransfer über die Grenzen nicht erlaubt oder stark

¹⁴ Siehe Fussnote 1.

einschränkt. Die EBK beschloss, auch diese Bestimmung beizubehalten. Da Reputationsrisiken keine Landesgrenzen kennen, müssen die verantwortlichen Organe der Gruppe wesentliche Geschäftsbeziehungen, mit welchen erhöhte Risiken verbunden sind, kennen. Zu diesem Zweck muss ein Transfer von den dafür wesentlichen Informationen in beide Richtungen möglich sein, und zwar von der ausländischen Gruppengesellschaft zur schweizerischen Muttergesellschaft als auch umgekehrt. Die EBK war sich des Bestehens allfälliger Hindernisse beim grenzüberschreitenden Informationsfluss durchaus bewusst, weshalb sie für den Fall, dass die erforderlichen Informationen im Ausland nicht zugänglich sein sollten, eine entsprechende Informationspflicht einführte. Für schweizerische Zweigniederlassungen und Gruppengesellschaften ausländischer Banken lehnt sich diese Bestimmung an Art. 4^{quinquies} des Bankengesetzes, wonach alle für die konsolidierte Aufsicht erforderlichen Informationen an die ausländische Muttergesellschaft übermittelt werden dürfen.

- Die im Vernehmlassungsentwurf vorgesehene Ausweitung des PEP-Begriffs auf ehemalige PEP fand bei den Vernehmlassungsteilnehmern keine breite Unterstützung. Um Personen mit prominenten öffentlichen Funktionen nicht auf Lebenszeit als PEP zu kategorisieren, verzichtet die Verordnung auf diese Ausweitung. Um den Geltungsbereich der PEP-Regelung nicht übermässig auszudehnen, was wiederum gegen ein risikoorientiertes Vorgehen spricht, verzichtet die Verordnung, entgegen den Wünschen einiger Vernehmlassungsteilnehmer, darauf, alle inländischen PEP derselben Regelung zu unterwerfen. Personen mit prominenten öffentlichen Funktionen auf regionaler Ebene sowie Parlamentarier werden ebenfalls nicht von der PEP-Definition erfasst. Hingegen gelten die allgemeinen Grundsätze der Geldwäschereiprävention der GwV-EBK, namentlich das allgemeine Verbot der Annahme von Vermögenswerten aus Korruption und anderen Verbrechen. Die Verordnung verlangt von allen Finanzintermediären die Entwicklung von Kriterien, welche

auf Geschäftsbeziehungen mit erhöhten Rechts- oder Reputationsrisiken hinweisen, und gibt eine nicht abschliessende Aufzählung möglicher Kriterien. In Anwendung dieser Kriterien können auch Geschäftsbeziehungen mit inländischen PEP als mit erhöhten Risiken behaftet eingestuft werden. Im Unterschied zu Geschäftsbeziehungen mit ausländischen PEP ist diese Einordnung jedoch nicht zwingend. Es ist einem Finanzintermediär unbenommen, für sich selbst gewisse oder alle inländischen PEP der Kategorie erhöhter Risiken zuzuordnen und zusätzliche Sorgfaltspflichten anzuwenden. Führt ein inländischer PEP eine Transaktion aus, welche den Umständen nach als ungewöhnlich erkannt wird, ist wie auch bei allen ungewöhnlichen Transaktionen eine zusätzliche Sorgfalt anzuwenden.

- Zahlreiche Vernehmlassungsteilnehmer äusserten Bedenken gegenüber der Pflicht zur Angabe von Name und Kontonummer des Auftraggebers bei Zahlungsaufträgen. Die Vertreter der Banken sehen erhebliche Sicherheitsrisiken, sollten Name und Kontonummer des Auftragsgebers auf Transaktionsbelegen angegeben werden müssen. Insbesondere bei einer Abwicklung über mehrere Korrespondenzbanken bestände ihrer Ansicht nach eine Gefahr des Missbrauchs dieser Informationen (identity fraud), da Kontonummer und Name des Kontoinhabers einer weit grösseren Zahl von Beteiligten bekannt gegeben werden. Die Verordnung trägt diesen Sicherheitsbedenken dadurch Rechnung, dass sie auch die Angabe einer Identifizierungsnummer anstelle der Kontonummer zulässt.
- Verschiedene Vernehmlassungsteilnehmer sprachen sich gegen die von der EBK geforderte Pflicht zu einem persönlichen Kontakt mit dem Kunden aus, da dieser in einzelnen Geschäftsbereichen (z.B. E-Banking) sowie bei manchen ausländischen Kunden nicht möglich sei. Statt eine allgemeine Pflicht zum persönlichen Kontakt einzuführen, nimmt die Verordnung den fehlenden persönlichen Kundenkontakt nunmehr als ein weiteres Kriterium für Geschäftsbeziehungen mit erhöhten Risiken auf, welche zusätzlichen Abklärungen unterliegen.

- Als einer der Hauptkritikpunkte erwies sich die Frage der Übergangsfrist. Zahlreiche Vernehmlassungsteilnehmer sprachen sich gegen die von der EBK geforderte Verkürzung der einjährigen Übergangsfrist aus und forderten stattdessen insbesondere für die Einteilung bestehender Geschäftsbeziehungen in Risikokategorien sowie die Einführung eines Transaktionsüberwachungssystems eine Verlängerung. Die EBK verzichtete auf eine Verkürzung der Übergangsfrist, sah jedoch von einer Fristverlängerung ab, da sie einzelnen Finanzintermediären auf ein begründetes Gesuch hin eine Fristverlängerung gewähren kann.

Bei der Ausarbeitung der vorliegenden Fassung der Verordnung, welche am 18. Dezember 2002 von der EBK beschlossen wurde, wurde der Mehrzahl der Stellungnahmen und Detailvorschläge der Vernehmlassungsteilnehmer Rechnung getragen. Die in der Verordnung gegenüber dem Vernehmlassungsentwurf aufgenommenen Modifikationen ändern jedoch nichts an den zentralen Neuerungen gegenüber der geltenden Ordnung.¹⁵

3 Nationale Rahmenbedingungen

Die Verordnung der EBK ist nur eine der Säulen des schweizerischen Abwehrdispositivs gegen Geldwäscherei und Terrorismusfinanzierung, das sich aus einer präventiven verwaltungsrechtlichen Komponente und einer repressiven strafrechtlichen Komponente zusammensetzt. Die Weiterentwicklung der Regulierung der EBK steht daher in einem engen Zusammenhang mit den gesetzgeberischen und institutionellen Entwicklungen, welche in der Schweiz in den letzten Jahren im Bereich der Geldwäschereibekämpfung erfolgt sind und hiernach beschrieben werden.

¹⁵ Für eine Aufführung der wichtigsten Änderungen gegenüber dem Vernehmlassungsentwurf siehe Anhang I.

3.1 Entwicklungen in der Gesetzgebung

Seit Anfang der achtziger Jahre wurden auf nationaler Ebene eine Reihe straf-, aufsichts- und standesrechtlicher Bestimmungen zur Verbesserung der Geldwäschereibekämpfung geschaffen. Im Bereich des Strafrechts sind seit dem 1. August 1990 die Bestimmungen des Strafgesetzbuches¹⁶ betreffend Geldwäscherei und mangelnde Sorgfalt bei Finanzgeschäften in Kraft. Als Geldwäscherei werden alle Handlungen geahndet, welche die Ermittlung der Herkunft, Auffindung oder Einziehung von Vermögenswerten, die aus einem Verbrechen herrühren, vereiteln sollen.¹⁷ Die mangelnde Sorgfalt bei Finanzgeschäften erfasst insbesondere die Unterlassung der Feststellung der Identität des wirtschaftlich Berechtigten.¹⁸ Das im August 1994 eingeführte Melderecht berechtigt alle Finanzintermediäre, den Behörden Informationen und Wahrnehmungen zu melden, die darauf schliessen lassen, dass Vermögenswerte aus einem Verbrechen herrühren.¹⁹

Neben den erwähnten Bestimmungen haben auch andere Strafnormen Geldwäschereirelevanz, und zwar als Vortaten zu den Verstössen gegen das Geldwäschereigesetz. In diesem Zusammenhang sind die am 1. August 1994 in Kraft getretenen Bestimmungen zur Bekämpfung des organisierten Verbrechens²⁰ sowie das Korruptionsstrafrecht zu erwähnen²¹, wobei neu in Umsetzung des OECD-Übereinkommens über die Bekämpfung der Bestechung ausländischer Amtsträger im internationalen Geschäftsverkehr²² auch die Bestechung ausländischer Amtsträger unter Strafe gestellt wird.²³

Die neu in das Strafgesetzbuch aufgenommene Verantwortlichkeit von Unternehmen ist gleichermassen von Bedeutung für die Ahndung der

¹⁶ Schweizerisches Strafgesetzbuch vom 21.12.1937 (SR 311.0), verfügbar im Internet unter http://www.bk.admin.ch/ch/d/sr/c311_0.html.

¹⁷ Art. 305^{bis} StGB.

¹⁸ Art. 305^{ter} StGB.

¹⁹ Art. 305^{ter} Absatz 2 StGB.

²⁰ Art. 260^{bis} Ziff.1 StGB.

²¹ Siehe Art. 322^{quater} (aktive Bestechung) und Art. 322^{ter} (passive Bestechung) StGB.

²² Siehe Fussnote 62.

²³ Art. 322^{septies} StGB.

Geldwäscherei.²⁴ Sie statuiert eine Haftbarkeit des Unternehmens wegen Organisationsverstössen in zwei Fällen: Primär, wenn das Unternehmen bei spezifischen Straftaten nicht alle erforderlichen und zumutbaren Vorkehren zu deren Verhinderung getroffen hat; subsidiär – bei gemeinen Vergehen oder Verbrechen –, wenn die Straftat keiner natürlichen Person innerhalb des Unternehmens wegen mangelhafter Organisation seinerseits zugeordnet werden kann. Zur Umsetzung der Terrorismusfinanzierungskonvention soll eine spezielle Strafnorm zur Terrorismusfinanzierung geschaffen werden.²⁵

Das am 1. April 1998 in Kraft getretene Geldwäschereigesetz²⁶ ergänzt die erwähnten Bestimmungen des Strafgesetzes. Der Geltungsbereich des Geldwäschereigesetzes erstreckt sich über den gesamten Finanzsektor. Das Gesetz knüpft am Begriff des Finanzintermediärs an und erfasst damit neben den bereits vor Erlass des Gesetzes spezialgesetzlich beaufsichtigten Finanzintermediären wie Banken, Versicherungen, Effektenhändler und Fondsleitungen nun insbesondere auch Treuhandgesellschaften, Vermögensverwalter, Anwälte und Notare, die Post, Edelmetallhändler und Wechselstuben. Das Gesetz auferlegt den Finanzintermediären Verpflichtungen organisatorischer Art, beispielsweise betreffend die Ausbildung des Personals und interne Kontrollen, sowie Verpflichtungen funktioneller Art, wie die Identifizierung der Vertragspartei, die Feststellung des wirtschaftlich Berechtigten, die Abklärung der wirtschaftlichen Hintergründe einer Transaktion bei Anhaltspunkten auf Geldwäscherei und die Aufbewahrungspflicht für Belege. Für die Banken brachte das Geldwäschereigesetz hinsichtlich dieser Pflichten keine Änderungen, da im Bankensektor diese Pflicht-

²⁴ Siehe Art. 102 und 102a neuStGB, Schweizerisches Strafgesetzbuch: Änderung vom 13. Dezember 2002, auf dem Internet verfügbar unter <http://www.ofj.admin.ch/d/index.html>, siehe auch Botschaft zur Änderung des Schweizerischen Strafgesetzbuches (Allgemeine Bestimmungen, Einführung und Anwendung des Gesetzes) und des Militärstrafgesetzes sowie zu einem Bundesgesetz über das Jugendstrafrecht vom 21. September 1998 (BB1 1999 1979).

²⁵ Siehe Ziff. 4.2 und 5.8 hiernach.

²⁶ Bundesgesetz zur Bekämpfung der Geldwäscherei im Finanzsektor vom 10.10.1997 (GwG; SR 955.0) verfügbar im Internet unter <http://www.bk.admin.ch/ch/d/sr/9/955.0.de.pdf>.

ten zum Teil bereits in der Sorgfaltspflichtvereinbarung²⁷ und zum Teil durch die Geldwäschereirichtlinien der EBK²⁸ präzisiert worden sind.

3.2 Institutioneller Rahmen

Das Geldwäschereigesetz schafft zwei neue Bundesbehörden, die zu den bisherigen spezialgesetzlichen Aufsichtsbehörden hinzukommen und die Durchführung der geschaffenen Kontrollmechanismen gewährleisten sollen: die Kontrollstelle²⁹ und die Meldestelle³⁰. Das Geldwäschereigesetz überträgt staatliche Kontrollaufgaben an private Selbstregulierungsorganisationen.³¹

Die Kontrollstelle ist organisatorisch der Eidgenössischen Finanzverwaltung angegliedert. Ihr unterstehen alle Finanzintermediäre, ausgenommen jene, die spezialgesetzlich durch die EBK oder das Bundesamt für Privatversicherungen beaufsichtigt werden. Die Finanzintermediäre müssen einer Selbstregulierungsorganisation beitreten oder sich direkt der Aufsicht durch die Kontrollstelle unterstellen. Im ersten der beiden Fälle übt die Kontrollstelle über die Selbstregulierungsorganisationen eine indirekte Aufsicht aus. Bei Verletzung der im Geldwäschereigesetz aufgestellten Pflichten können Selbstregulierungsorganisationen gegen ihre Mitglieder Konventionalstrafen verhängen. Die Kontrollstelle kann Massnahmen gegen die Selbstregulierungsorganisationen und die ihr direkt unterstellten Finanzintermediäre ergreifen und ihnen im Ernstfall die Anerkennung oder Bewilligung entziehen und die Liquidation des Finanzintermediärs anordnen.

Ausser den eigentlichen Sorgfaltspflichten sieht das Geldwäschereigesetz die Pflicht vor, bei begründetem Verdacht auf Geldwäscherei

²⁷ Siehe Fussnote 38.

²⁸ EBK-Rundschreiben 91/3 Richtlinien zur Bekämpfung der Geldwäscherei vom 18. Dezember 1991, siehe auch EBK-Jahresbericht 1991, S. 33 ff. Das Rundschreiben wurde durch das EBK-Rundschreiben 98/1 vom 26. März 1998 ersetzt, das seit dem 1. Juli 1998 in Kraft ist.

²⁹ Art. 17–22 GwG, siehe auch die Website der Kontrollstelle unter <http://www.gwg.admin.ch>.

³⁰ Art. 23 GwG, siehe auch die Website der Meldestelle unter http://internet.bap.admin.ch/d/themen/geld/i_index.htm.

³¹ Art. 24–28 GwG.

der Meldestelle für Geldwäscherei Meldung zu erstatten und die involvierten Vermögenswerte zu sperren. Die durch das Geldwäschereigesetz eingesetzte Meldestelle ist dem Bundesamt für Polizei angegliedert. Ihre Aufgabe besteht darin, die ihr von den Finanzintermediären in Anwendung des Geldwäschereigesetzes gemeldeten Informationen zu sammeln und auszuwerten. Bei begründetem Verdacht auf Geldwäscherei zeigt sie dies unverzüglich den zuständigen Strafverfolgungsbehörden an. Die Ermittlungskompetenz im Bereich der Geldwäscherei sowie auch der organisierten Kriminalität, Korruption und schweren Wirtschaftskriminalität wurde im Rahmen der sogenannten Effizienzvorlage dem Bund übertragen.³²

3.3 Aufsichtsrecht und die Rolle der EBK

Der EBK obliegt es, die Einhaltung der vom Geldwäschereigesetz vorgeschriebenen Pflichten bei den ihrer Aufsicht unterstellten Instituten zu überwachen. Einzelne dieser Sorgfaltspflichten, beispielsweise das Gebot, bei schwierigen, grossen und ungewöhnlichen Transaktionen den wirtschaftlichen Hintergrund abzuklären³³, hat die EBK bereits Ende der 70er Jahre einzelfallweise gestützt auf das bankengesetzliche Gebot der einwandfreien Geschäftstätigkeit³⁴ angewendet. Im Zusammenhang mit dem Fall Marcos entwickelte die EBK ihre Praxis, wonach die Geschäftsleitung und nicht untergeordnete Stellen in einer Bank darüber zu entscheiden haben, ob eine Geschäftsbeziehung mit einer politisch exponierten Person aufgenommen oder weitergeführt werden soll. Diese Praxis wurde erstmals im Jahresbericht 1987 veröffentlicht³⁵ und im Nachgang zu den Fällen Mobutu und Benazir Bhutto im Verlauf des Jahres 1997 noch weiter verfeinert.³⁶ Anlässlich der

³² Schweizerisches Strafgesetzbuch (Schaffung neuer Verfahrenskompetenzen des Bundes in den Bereichen organisiertes Verbrechen und Wirtschaftskriminalität), Änderung vom 22. Dezember 1999, verfügbar auf dem Internet unter <http://www.bk.admin.ch/ch/d/as/2001/3071.pdf>. Die Regelung ist seit dem 1. Januar 2002 in Kraft.

³³ BGE 111 Ib 126.

³⁴ Art. 3 Abs. 2 Bst. c BankG.

³⁵ EBK-Jahresbericht 1987, S. 29 f.

³⁶ EBK-Jahresbericht 1997, S. 20 ff.

Überarbeitung ihrer Geldwäschereirichtlinien im Jahre 1998, die der Anpassung an die Bestimmungen des Geldwäschereigesetzes diene, verankerte die EBK diese Regeln im neuen Rundschreiben. Jüngste Anwendungsfälle dieser Regeln, insbesondere des Erfordernisses, die wirtschaftlichen Hintergründe und den Zweck von Geschäftsbeziehungen sowie die mögliche PEP-Eigenschaft von Kunden sorgfältig abzuklären und dazu auch aktiv öffentliche Informationsquellen zu konsultieren, sind die Fälle Abacha und Montesinos.³⁷

Die EBK kann gegen einzelne Verantwortliche verwaltungsrechtliche Massnahmen ergreifen und ihnen beispielsweise verbieten, im Bankensektor vergleichbare Funktionen wahrzunehmen. Stellt sie organisatorische Schwachstellen bei überwachten Instituten hinsichtlich der «legal and compliance»-Funktionen fest, werden die betroffenen Institute angewiesen, diese unter enger aufsichtsrechtlicher Kontrolle in kurzer Frist zu beheben. Bei systematischer Verletzung und Organisationsmängeln ist ein Bewilligungsentzug möglich. In den jüngsten Fällen hat die EBK über die Resultate ihrer Untersuchungen und die angeordneten Massnahmen öffentlich berichtet.

3.4 Selbstregulierung der Banken

Die Identifizierung von Bankkunden ist bereits seit 1977 durch die Banken selbst in der seither mehrfach überarbeiteten VSB³⁸ geregelt. Im Rahmen der staatlichen Geldwäschereigesetzgebung hat die VSB gestützt auf Art. 16 des Geldwäschereigesetzes die zusätzliche Funktion übernommen, die Sorgfaltspflichten zu konkretisieren. Aufgabe der Bankenkommission als spezialgesetzliche Aufsichtsbehörde ist es zu prüfen, ob die VSB die Erfüllung der im Geldwäschereigesetz enthaltenen Pflichten ausreichend regelt. Die externen Revisoren haben den Auftrag, die Einhaltung der VSB zu überprüfen. Über die Einhal-

³⁷ Siehe Bericht der EBK «Abacha-Gelder bei Schweizer Banken», publiziert auf der Website der EBK (<http://www.ebk.admin.ch/d/archiv/2000/neu14a-00.pdf>) und Medienmitteilung vom 13. November 2001 im Fall Montesinos (<http://www.ebk.admin.ch/d/aktuell/m1113-01d.pdf>).

³⁸ Verfügbar auf dem Internet unter http://www.swissbanking.org/110_d.pdf.

tung der Standesregeln wacht zudem eine von der SBVg auf fünf Jahre gewählte Aufsichtskommission, welche auf Antrag der ebenfalls von der SBVg eingesetzten Untersuchungsbeauftragten entscheidet. Wo sie Standesregelverletzungen feststellt, kann die Aufsichtskommission Konventionalstrafen verhängen. Die Aufsichtskommission veröffentlicht regelmässig einen Tätigkeitsbericht über ihre Praxis.³⁹

Zeitgleich mit der Überarbeitung der Geldwäschereiregelung wurde auch die VSB aus dem Jahr 1998 überarbeitet.⁴⁰ Am 1. Juli 2003 tritt die vorliegende sechste Fassung (VSB 03) in Kraft.

4 Internationale Entwicklungen

In den letzten Jahren arbeiteten verschiedene internationale Gremien Standards zur Geldwäschereibekämpfung aus. Die Terroranschläge gegen die Vereinigten Staaten vom 11. September 2001 führten zu einer weiteren Ausweitung des Kampfes gegen die Geldwäscherei und zur Verabschiedung von internationalen Empfehlungen zur Bekämpfung der Terrorismusfinanzierung. Die Einhaltung internationaler Mindeststandards wird nunmehr regelmässig im Rahmen von Länderprüfungen, wie den Mutual Self-Assessments der Financial Action Task Force on Money Laundering (FATF)⁴¹ oder dem Financial Sector Assessment Program (FSAP) des Internationalen Währungsfonds (IWF)⁴², von internationalen Experten geprüft. Es ist daher wichtig, bei der Ausarbeitung der nationalen Regulierung im Bereich der Geldwäscherei und Terrorismusbekämpfung die internationalen Rahmenbe-

³⁹ «Übersicht über die Praxis der Aufsichtskommission zur Sorgfaltspflicht der Banken 1998–2001», verfügbar auf dem Internet unter http://www.swissbanking.org/auf_sorg_d_ber.pdf.

⁴⁰ Vgl. Ziff. 6 hiernach.

⁴¹ Die FATF ist ein unabhängiges internationales Gremium, dessen Sekretariat bei der OECD angesiedelt ist. Die 29 Mitgliedsländer und Regierungen der FATF sind: Argentinien, Österreich, Belgien, Brasilien, Kanada, Dänemark, Finnland, Frankreich, Deutschland, Griechenland, Hongkong, China, Island, Irland, Italien, Japan, Luxemburg, Mexiko, Niederlande, Neuseeland, Norwegen, Portugal, Singapur, Spanien, Schweden, Schweiz, Türkei, Grossbritannien und die USA. Zwei internationale Organisationen sind ebenfalls Mitglieder der FATF: die Europäische Union und der arabische Golfat.

⁴² Siehe Ziff. 4.8.

dingungen zu berücksichtigen. Die wichtigsten internationalen Regelungsinstrumente werden nachfolgend aufgeführt.

4.1 Die 40 FATF-Empfehlungen (Juni 1996)

Die 40 Empfehlungen der FATF vom 7. Februar 1990, welche am 28. Juni 1996 geändert wurden⁴³, bilden heute einen international anerkannten Standard für Massnahmen, die ein Land zur wirksamen Bekämpfung der Geldwäscherei ergreifen muss. Die Empfehlungen definieren Minimalanforderungen für die Identifizierung von Kunden und die Aufbewahrung von Unterlagen, eine erhöhte Sorgfalt bei der Feststellung und Meldung verdächtiger Transaktionen sowie Massnahmen für den Verkehr mit Ländern, die ungenügende Vorkehrungen zur Bekämpfung der Geldwäscherei getroffen haben. Die FATF sieht vor, bis Mitte 2003 eine überarbeitete Fassung der Empfehlungen zu verabschieden. Ein entsprechendes Konsultationspapier ist im Mai 2002 publiziert worden.⁴⁴

Auf der Grundlage der Empfehlungen der FATF entwickelten der IWF und die Weltbank eine Methodologie⁴⁵, welche Kriterien zur Beurteilung der Einhaltung und Umsetzung der geldwäschereirelevanten Bestimmungen, insbesondere der FATF-Empfehlungen, formuliert. Diese Methodologie soll Prüfern im Rahmen von Evaluationen durch den IWF, die Weltbank und die FATF als Hilfsmittel bei der Beurteilung der Geldwäschereisysteme einzelner Länder dienen.

4.2 FATF-Empfehlungen gegen die Terrorismusfinanzierung (Oktober 2001)

An ihrer ausserordentlichen Vollversammlung in Washington im Oktober 2001 verabschiedete die FATF ein Sofortprogramm, mit dem alle

⁴³ EBK-Bulletin 31, S. 19 ff.; siehe auch unter http://www1.oecd.org/fatf/pdf/40Rec_de.pdf.

⁴⁴ Verfügbar auf dem Internet: http://www.fatf-gafi.org/pdf/Review40_en.pdf.

⁴⁵ Fund and Bank Methodology for Assessing Legal, Institutional and Supervisory Aspects of Anti-Money Laundering and Combating the Financing of Terrorism (AML/CFT Methodology) 2002, verfügbar auf dem Internet unter <http://www.imf.org/external/np/mae/aml/2002/eng/110802.pdf>.

Länder der Welt dazu angehalten werden, den neuen internationalen Empfehlungen gegen die Terrorismusfinanzierung unverzüglich nachzukommen.⁴⁶ Diese Empfehlungen sehen namentlich vor, dass alle Staaten die Pflicht zur Erstattung von Verdachtsanzeigen auf die Terrorismusfinanzierung ausweiten, im internationalen elektronischen Zahlungsverkehr (Wire Transfers) Kundenidentifizierungspflichten durchsetzen und sicherstellen, dass Unternehmen, insbesondere gemeinnützige Vereinigungen, nicht zur Finanzierung des Terrorismus missbraucht werden.⁴⁷

4.3 Terrorismusfinanzierungskonvention (Dezember 1999)

Die Ratifizierung und Umsetzung des internationalen Übereinkommens zur Bekämpfung der Finanzierung des Terrorismus vom 9. Dezember 1999⁴⁸ bildet Gegenstand einer der FATF-Empfehlungen gegen die Terrorismusfinanzierung. Die Terrorismusfinanzierungskonvention legt die Terrorismusfinanzierung als eigenständiges Delikt fest, d.h. eine Bestrafung kann unabhängig davon erfolgen, ob der eigentliche Terrorakt tatsächlich ausgeführt wird oder nicht. Des Weiteren enthält die Konvention Bestimmungen, welche die internationale Zusammenarbeit erleichtern und die Vorbereitung und Durchführung finanzieller Aktivitäten zu Gunsten des Terrorismus vereiteln sollen. Der Bundesrat beschloss im November 2001, die Terrorismusfinanzierungskonvention zu ratifizieren, und unterbreitete am 26. Juni 2002 dem Parlament eine entsprechende Botschaft mitsamt einem Entwurf für die notwendigen Anpassungen des Strafgesetzbuches.⁴⁹ Im Zentrum der Strafrechtsrevision steht eine Strafnorm der Terrorismusfinanzierung.

⁴⁶ Financial Action Task Force on Money Laundering, Special Recommendation on Terrorist Financing, 31 October 2001, verfügbar auf dem Internet unter http://www1.oecd.org/fatf/SRecsTF_en.htm.

⁴⁷ Als ein Hilfsinstrument zur Entdeckung von Verbindungen zu Terrorismusorganisationen und der Terrorismusfinanzierung hat die FATF Weisungen («Guidance for Financial Institutions in Detecting Terrorist Financing») veröffentlicht. Sie sind auf dem Internet unter http://www1.oecd.org/fatf/pdf/GuidFITF01_en.pdf abrufbar.

⁴⁸ International Convention for the Suppression of the Financing of Terrorism A/RES/54/109 <http://untreaty.un.org/English/Terrorism/Conv12.pdf>.

⁴⁹ Die Botschaft ist auf dem Internet verfügbar unter <http://www.bk.admin.ch/ch/d/ff/2002/5390.pdf>; siehe auch unter Ziff. 5.8.

Weiter soll die Bestimmung über die Verantwortlichkeit des Unternehmens, die bereits im Rahmen der Revision des Allgemeinen Teils des Strafgesetzbuches von Dezember 2002 aufgenommen wurde, auf die neuen terroristischen Straftaten ausgedehnt werden.

4.4 Wolfsberg-Prinzipien (2000/2002)

Im Oktober 2000 einigte sich eine Gruppe weltweit führender Banken auf globale Richtlinien zur Bekämpfung der Geldwäscherei für international tätige Privatbanken. Die Prinzipien befassen sich mit verschiedenen Aspekten des «know your customer»-Prinzips beim Verkehr zwischen vermögenden Privatkunden und Private-Banking-Abteilungen der Finanzinstitute sowie der Erkennung und Verfolgung ungewöhnlicher oder verdächtiger Aktivitäten. Im Januar 2002 beschloss die Gruppe der Banken die Wolfsberg-Prinzipien auf die Terrorismusbekämpfung auszudehnen.⁵⁰ Sie wurden im Mai 2002 von der Wolfsberg-Gruppe revidiert und erfuhren in einzelnen Punkten Präzisierungen.⁵¹ Im November 2002 wurden Prinzipien zu den anwendbaren Sorgfaltspflichten bei Korrespondenzbankenbeziehungen verabschiedet.⁵² Ihnen wie auch den ursprünglichen Prinzipien zur Bekämpfung der Geldwäscherei liegt ein risikoorientierter Ansatz zugrunde.

4.5 «Customer Due Diligence Paper» des Basler Ausschusses (Oktober 2001)

Ende 2001 verabschiedete der Basler Ausschuss für Bankenaufsicht⁵³ die von einer Arbeitsgruppe mit Vertretern des Basler Ausschusses und

⁵⁰ Wolfsberg Statement on the suppression of the financing of terrorism, Januar 2002, verfügbar auf dem Internet <http://www.wolfsberg-principles.com>.

⁵¹ Auf dem Internet verfügbar (http://www.wolfsberg-principles.com/wolfsberg_principles_1st_revision).

⁵² Erhältlich unter http://www.wolfsberg-principles.com/wolfsberg_principles_correspondent.html.

⁵³ Der Basler Ausschuss für Bankenaufsicht wurde Ende 1974 von den Zentralbank-Gouverneuren der Zehnergruppe (G10) bei der Bank für Internationalen Zahlungsausgleich (BIZ) in Basel gegründet. Der Ausschuss setzt sich aus Vertretern der Zentralbanken und Bankaufsichtsbehörden folgender 13 Länder zusammen: Belgien, Deutschland, Frankreich, Italien, Japan, Kanada, Luxemburg, Niederlande, Schweden, Schweiz, Spanien, Vereinigtes Königreich und USA.

der Vereinigung der Aufsichtsbehörden von Offshore-Finanzplätzen formulierten Mindeststandards zur Kundenidentifizierung. Dieses Dokument gibt dem neusten internationalen Standard für die Sorgfaltspflichten von Banken Ausdruck und ergänzt die Grundsätze für eine wirksame Bankenaufsicht vom September 1997 (insbesondere Grundsatz 15 betreffend die Kundenidentifizierung).⁵⁴ Es ist wie alle Texte des Basler Ausschusses nicht verbindlich, bildet aber dennoch einen neuen Minimalstandard, mit dem sich alle Mitglieder des Ausschusses einverstanden erklärten. Die Mindeststandards verlangen, dass bei international tätigen Bankkonzernen die Verfahren zur Feststellung der Kundenidentität und das Risikomanagement konzernweit konsolidiert werden. International tätige Finanzgruppen müssen ihre Rechts- und Reputationsrisiken global erfassen, begrenzen und überwachen. Im Nachgang zu den Ereignissen des 11. Septembers 2001 gewann dieser Grundsatz weiter an Bedeutung. An einer Konferenz von Rechtsexperten der G10-Staaten zum Informationsaustausch über die Bekämpfung der Terrorismusfinanzierung wurde die Notwendigkeit einer engeren Zusammenarbeit zwischen den Aufsichtsbehörden einerseits sowie das Erfordernis eines zentralisierten Risikomanagementsystems bei international tätigen Bankgruppen andererseits in einem gemeinsamen Papier bekräftigt.⁵⁵

4.6 «Supervisors' PEP working paper 2001» (November 2001)

Auf Initiative der Schweiz fand im November 2000 in Lausanne eine Tagung zum Umgang mit Geschäftsbeziehungen mit PEP statt. Vertreter von Justiz- und Bankenaufsichtsorganen der G7-Staaten und der Schweiz setzten sich grundsätzlich mit der PEP-Problematik auseinander und diskutierten die Erkenntnisse aus dem Fall Abacha. Die im

⁵⁴ Customer due diligence for banks (<http://bis.org/publ/bcbs85.htm>. Grundsätze für eine wirksame Bankaufsicht, publiziert in EBK-Bulletin 33, S. 73 ff.

⁵⁵ Sharing of financial records between jurisdictions in connection with the fight against terrorist financing, Summary of a meeting of representatives of Supervisors and Legal Experts of G10 Central Banks and Supervisory Authorities on 14 December 2001, Basel, Switzerland, verfügbar unter <http://www.bis.org/publ/bcbs89.pdf>.

Anschluss an das Treffen durch Vertreter der Aufsichtsbehörde von G7-Ländern und der Schweiz erarbeiteten Empfehlungen zur Entgegennahme von Vermögenswerten von Personen mit bedeutenden öffentlichen Funktionen («Supervisors' PEP working paper 2001»)⁵⁶ wurden im November 2001 fertig gestellt. Das Dokument stellt eine Grundlage für eine Reglementierung von Geschäftsbeziehungen zu Personen mit bedeutenden öffentlichen Aufgaben dar, wie sie auch in diese Verordnung einfließt.

4.7 Weitere wichtige internationale Rechtsinstrumente

Als weitere wichtige internationale Rechtsinstrumente auf dem Gebiet der Bekämpfung der Geldwäscherei und Terrorismusfinanzierung sind zu nennen: die Europäische Geldwäschereirichtlinie vom 10. Juni 1991 (erweitert um die Richtlinie 2001/97 vom 4. November 2001)⁵⁷, das zweite Protokoll zum Übereinkommen über den Schutz der finanziellen Interessen der Europäischen Gemeinschaften⁵⁸, der Rahmenbeschluss des Rates vom 26. Juni 2001 über Geldwäsche sowie Ermittlung, Einfrieren, Beschlagnahme und Einziehung von Tatwerkzeugen und Erträgen aus Straftaten⁵⁹, das Wiener Übereinkommen der Vereinten Nationen vom 19. Dezember 1988⁶⁰, das Übereinkommen des Europarates vom 8. November 1990 über Geldwäsche sowie die Ermitt-

⁵⁶ Verfügbar unter <http://www.ebk.admin.ch/d/aktuell/neu090702-03d.pdf>.

⁵⁷ Richtlinie +91/308/EWG des Rates vom 10. Juni 1991 zur Verhinderung der Nutzung des Finanzsystems zum Zwecke der Geldwäsche (Amtsblatt Nr. L 166 vom 28.6.1991, S. 77 ff.) und Richtlinie 2001/97/EG des Europäischen Parlaments und des Rates vom 4. Dezember 2001 zur Änderung der Richtlinie 91/308/EWG des Rates zur Verhinderung der Nutzung des Finanzsystems zum Zwecke der Geldwäsche (Amtsblatt Nr. L 344 vom 28.12.2001, S. 0076 – 0082). Mit der Änderung der Geldwäscherichtlinie (91/308/EWG) wurde der Begriff der Geldwäscherei auf alle Erträge ausgedehnt, die aus schweren Straftaten stammen, während die ursprüngliche Richtlinie dies nur für Erträge aus Drogendelikten vorschrieb. Zudem wird mit der neuen Richtlinie der Geltungsbereich der (auf den Finanzsektor beschränkten) ursprünglichen Richtlinie auf eine Reihe nichtfinanzieller Tätigkeiten und Berufe ausgedehnt, die Geldwäscher leicht für ihre Zwecke missbrauchen können, namentlich Immobilienmakler, Notare, Rechtsanwälte, Kunsthändler, Auktionäre und Casinos.

⁵⁸ Amtsblatt Nr. C 221 vom 19.7.1997, S. 12 ff.

⁵⁹ Amtsblatt Nr. L 182 vom 5.7.2001, S. 1 f.

⁶⁰ United Nations Convention against illicit traffic in narcotic drugs and psychotropic substances, verfügbar auf dem Internet unter <http://www.incb.org/e/conv/1988/index.htm>.

lung, Beschlagnahme und Einziehung von Erträgen aus Straftaten⁶¹, das OECD-Übereinkommen über die Bekämpfung der Bestechung ausländischer Amtsträger im internationalen Geschäftsverkehr vom 21. November 1997⁶², die Strafrechtskonvention des Europarates gegen Korruption vom 27. Januar 1999⁶³ sowie die UNO-Konvention gegen das länderübergreifende organisierte Verbrechen⁶⁴ aus dem Jahr 2000.

4.8 IWF – Financial Sector Assessment Switzerland (Juni 2002)

Im Jahr 2001 führte der Internationale Währungsfonds in der Schweiz eine Finanzsektor-Länderevaluation (Financial Sector Assessment Program FSAP) durch.⁶⁵ Mittels standardisierter Fragebogen überprüfte der IWF die Befolgung von international anerkannten Standards und Kodizes zur Aufsicht der Banken, Börsen und Märkte, des Versicherungswesens und der Zahlungssysteme sowie zur Transparenz in den Bereichen Geld- und Finanzpolitik. Obwohl Ziel des FSAP primär die Analyse und Stärkung der Finanzsystemstabilität auf nationaler und internationaler Ebene ist, gehört auch die Geldwäschereibekämpfung zum Prüfungsfeld des FSAP. Der IWF entwickelte als Hilfsmittel für seine Assessments eine Methodologie, welche die geldwäscherei-relevanten internationalen Aufsichtsstandards zusammenfasst. Da zum Zeitpunkt der FSAP-Prüfungen die Arbeiten zu der Methodologie noch nicht abgeschlossen waren, erklärte sich die Schweiz zu einer ersten versuchsweisen Verwendung des Methodologieentwurfs im Rahmen des FSAP bereit. Die Schweizer Bestimmungen zur Bekämpfung der Geldwäscherei im Bankensektor bewertete der IWF als ange-

⁶¹ Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime, Strasbourg, 8. November 1990; am 11. Mai 1993 von der Schweiz unterzeichnet. Verfügbar auf dem Internet unter <http://Conventions.coe.int/treaty/en/Treaties/Html/141.htm>.

⁶² OECD-Übereinkommen über die Bekämpfung der Bestechung ausländischer Amtsträger im internationalen Geschäftsverkehr vom 17. Dezember 1997, verfügbar auf dem Internet unter <http://www.admin.ch/ch/d/ff/1999/5560.pdf>. Die Konvention wurde am 21. Mai 2000 von der Schweiz ratifiziert.

⁶³ Criminal Law Convention on Corruption, 27. Januar 1999, verfügbar auf dem Internet unter <http://conventions.coe.int/Treaty/EN/CadreListeTraites.htm>.

⁶⁴ United Nations Convention against transnational organized crime, verfügbar auf dem Internet unter http://www.uncjin.org/Documents/Conventions/dcatoc/final_documents_2/convention_eng.pdf.

⁶⁵ Vgl. EBK-Jahresbericht 2001, S. 24–26; EBK-Jahresbericht 2000, S. 32 f.

messen und im Einklang mit den internationalen Standards. In Bezug auf die Effektenhändler äusserte sich der IWF differenzierter, obwohl hier grundsätzlich dieselben Regeln zur Anwendung kommen. Kritisiert wurde insbesondere, dass die Identifizierung des wirtschaftlich Berechtigten nicht routinemässig erfolgen muss. Ein zusammenfassender Bericht des schweizerischen FSAP wurde im Juni 2002 publiziert.⁶⁶

5 Grundzüge der Verordnung

5.1 Verordnung an Stelle der Geldwäschereirichtlinien

Mit der Inkraftsetzung des Geldwäschereigesetzes am 1. April 1998 schufen Art. 16 Abs. 1 und Art. 41 des Geldwäschereigesetzes eine ausdrückliche gesetzliche Grundlage, die der EBK erlaubt, eine Verordnung zur Regelung dieses Bereichs zu erlassen. Mit dem Erlass einer Verordnung soll die Geldwäschereiregelung ein höheres Gewicht erhalten. Rechtstechnisch unterscheidet sich eine EBK-Verordnung von einem Rundschreiben in ihrer direkten Anwendbarkeit. Ein Rundschreiben stellt eine Auslegungshilfe dar und hat damit streng genommen im Gegensatz zur Verordnung, welche in der amtlichen Sammlung des Bundesrechts publiziert wird, keine materielle Rechtswirkung. De facto sind Rundschreiben und Verordnung jedoch gleichermaßen rechtsverbindlich. Die Wahl der Verordnung führt indes zu einer Straffung der Sprache, so dass trotz Aufnahme der Regelung aus der Notenhandelsrichtlinie sowie einer Reihe zusätzlicher Bestimmungen, wie beispielsweise zur Bekämpfung der Terrorismusfinanzierung, eine wesentlich kürzere Regulierung resultiert. Diese Regulierungstechnik entspricht auch derjenigen der Kontrollstelle für Geldwäscherei, welche die Sorgfaltspflichten der ihr direkt unterstellten Finanzintermediäre ebenfalls in einer Verordnung regelt. Die Geldwäschereiverordnung stellt eine Ergänzung des Geldwäschereigesetzes dar und wiederholt daher keine Bestimmungen, welche bereits im Geldwäschereigesetz enthalten sind.

⁶⁶ Verfügbar auf dem Internet unter <http://www.imf.org/external/pubs/ft/scr/2002/cr02108.pdf>.

5.2 Inhaltliche Abgrenzung zur Selbstregulierung

Die Geldwäschereirichtlinien enthalten heute keine Regeln zur Identifizierung der Vertragspartner und Feststellung der wirtschaftlich Berechtigten bei der Kontoeröffnung. Diese formalen und detaillierteren Vorschriften zur Konkretisierung der Artikel 3 bis 5 des Geldwäschereigesetzes sind in der durch die Bankiervereinigung im Dezember 2002 nun in der sechsten Fassung seit 1977 erlassenen Sorgfaltpflichtvereinbarung (VSB) enthalten. Die Bankenkommission hat diese Selbstregulierung als einen für alle Banken und Effektenhändler geltenden Mindeststandard anerkannt.⁶⁷ Demgegenüber regeln die geltenden Geldwäschereirichtlinien die organisatorischen Vorkehren zur Verhinderung der Geldwäscherei (Art. 7 und 8 GWG), geben Hinweise auf die Verhaltenspflichten bei ungewöhnlichen Transaktionen und Geschäftsbeziehungen (Art. 6 GwG) und präzisieren die Pflichten bei Geldwäschereiverdacht (Art. 9 und 10 GwG). Dabei ist die Regulierung der EBK allgemeiner gehalten als die Sorgfaltpflichtvereinbarung (VSB).

Die EBK erachtet dieses System nach wie vor für adäquat. Ohne die inhaltliche Abgrenzung ergäben sich zusätzliche Überlappungen im ohnehin schon komplizierten Normgefüge rund um die Geldwäschereibekämpfung. Zudem hält das Geldwäschereigesetz die Bankenkommission an, der Selbstregulierung Rechnung zu tragen (Art. 16 Abs. 1). Der im Vergleich zur Sorgfaltpflichtvereinbarung (VSB) geringere Detaillierungsgrad der Geldwäschereiverordnung ist sachlich gerechtfertigt, denn die Unterschiedlichkeit der Unternehmen, die der Aufsicht der EBK unterstellt sind, verlangt eine gewisse Flexibilität in der Umsetzung der Geldwäschereibestimmungen. Das Umsetzungskonzept eines jeden Finanzintermediärs muss auf die spezifischen Risiken des Finanzintermediärs, seine Grösse, seinen Kundenkreis und sein Dienstleistungsangebot zugeschnitten werden. Die Anforderungen der Geldwäschereiverordnung werden erst durch die Konkretisierung

⁶⁷ EBK RS 96/3 Anhang I.

in internen Weisungen und Compliance-Manuals des Finanzintermediärs operativ.

5.3 Entwicklung der Regeln über politisch exponierte Personen

Im Jahre 1998 traf die EBK im Nachgang zum Fall Mobutu den bewussten Entscheid, die bereits früher aufgestellten Regeln hinsichtlich der Behandlung von Geschäftsbeziehungen mit PEP, anlässlich der Revision des Rundschreibens aus dem Jahr 1991 ausdrücklich zu verankern und teilweise zu verfeinern. Diese Regelung bewährte sich grundsätzlich. Nicht zuletzt aufgrund der Publizität des Abacha-Falls wurde die Problematik auf Initiative der Schweiz hin inzwischen auch auf internationaler Ebene angegangen.⁶⁸ Mit der grösseren Aufmerksamkeit internationaler Gremien und der Medienöffentlichkeit stieg auch das mit der Annahme von Korruptionsgeldern verbundene Reputationsrisiko. Schliesslich schadet die Entgegennahme und Verwaltung von Korruptionsgeldern nicht nur dem Ruf des betroffenen Instituts, sondern auch dem Vertrauen der Öffentlichkeit in die ethischen Standards des Finanzplatzes als Ganzem.

Die Verfahren der EBK in den Fällen Abacha und Montesinos wiesen bei den betroffenen Instituten auf Schwachstellen bei der Abklärung von ungewöhnlichen Geschäftsbeziehungen hin und veranlassten die EBK, eine Verschärfung der Sorgfaltspflichten bei Geschäftsbeziehungen mit PEPs zu fordern. Die neue Verordnung verleiht den Regeln zum Umgang mit Geschäftsbeziehungen mit politisch exponierten Personen grössere Sichtbarkeit. Sowohl für Geschäftsbeziehungen mit politisch exponierten Personen wie auch für Geschäftsbeziehungen mit Personen, die vom Finanzintermediär selbst als mit erhöhten Risiken verbunden beurteilt werden, gelten nunmehr ausdrücklich zusätzliche Abklärungs- und Kontrollpflichten. Der Entscheid über die Aufnahme oder die Weiterführung von Geschäftsbeziehungen mit

⁶⁸ Siehe «Supervisors' PEP Working Paper 2001», Annex II des Berichts der Arbeitsgruppe KYC, Juni 2002, auf dem Internet verfügbar unter <http://www.ebk.admin.ch/d/archiv/2002/neu090702-03d.pdf>.

politisch exponierten Personen obliegt wie bisher dem obersten Geschäftsführungsorgan oder mindestens einem seiner Mitglieder.

5.4 Risikoorientierte Sorgfalt bei erhöhten Risiken

Die Verordnung verlangt zusätzlich zu den auf alle Kundenbeziehungen in gleicher Weise anwendbaren Kundenidentifizierungspflichten der VSB eine erhöhte Sorgfaltspflicht bei Geschäftsbeziehungen, die abstrakt höhere Risiken aufweisen. Die neue Regelung verlangt folglich keine höheren Sorgfaltspflichten bei der gesamten Kundschaft. Andererseits sind die höheren Anforderungen jedoch nicht auf PEP beschränkt.

Das erhöhte Risiko kann insbesondere durch den Wohnsitz des Kunden, seine berufliche Tätigkeit sowie die Art oder den Umfang seiner Transaktionen begründet werden. Die Finanzintermediäre haben selbst anhand von Merkmalen, die in der Verordnung beispielhaft aufgezählt werden, Kriterien zur Erfassung von Geschäftsbeziehungen mit erhöhten Risiken zu definieren. Dies setzt voraus, dass sie zuvor die spezifischen Risiken, die mit ihrer Geschäftstätigkeit und ihrem Kundenkreis verbunden sind, analysiert haben. Die Verordnung verzichtet darauf, eine abschliessende Liste von Risikokriterien aufzuführen, und ermöglicht damit den Finanzintermediären, die für ihre Geschäftsbereiche jeweils angemessenen Risikokriterien zu verwenden. Geschäftsbeziehungen mit höheren Risiken sollen vertieft abgeklärt werden, wobei verschiedene Quellen zu konsultieren sind. Ausserdem muss sich die oberste Geschäftsleitung auf eine direktere und systematischere Weise als bisher in die Überwachung dieser Geschäftsbeziehungen einschalten.

Das Konzept der risikoorientierten Aufsicht und Kontrolle ist nicht neu. Es liegt der Kontrolle von allen Risikoarten, traditionell vor allem von Markt- und Kreditrisiken, zugrunde und setzt eine eingehende Ri-

sikoanalyse voraus. Aus mangelnder Sorgfalt beim Eingehen und der Überwachung von Geschäftsbeziehungen können dem Finanzintermediär erhebliche Risiken erwachsen, namentlich Rechts- und Reputationsrisiken sowie operationelle Risiken und Konzentrationsrisiken⁶⁹, mit der Folge, dass dem Finanzintermediär durch gegen ihn gerichtete Forderungen, die Beschlagnahmung oder Sperrung von Aktiven sowie Kreditausfälle erhebliche finanzielle Kosten entstehen können.

5.5 Systematische Überwachung von Transaktionen

Die Verordnung führt die Verpflichtung ein, Transaktionen systematisch zu überwachen. Die fortlaufende Überwachung von Transaktionen ist eine wesentliche Komponente der Geldwäschereiprävention. Der Finanzintermediär soll sich dazu eines informatikgestützten Systems als Hilfsmittel bedienen. Die Informatik eröffnet umfangreiche Möglichkeiten einer automatischen Überwachung von Transaktionen.⁷⁰ Der Umfang der computergestützten Überwachung muss risikogerecht sein. Ein Finanzintermediär soll über ein System verfügen, das ihm hilft, ungewöhnliche oder verdächtige Vorgänge auf sämtlichen Konten aufzuspüren. Dies kann namentlich durch das Festlegen von Limiten für eine bestimmte Gruppe oder Kategorie von Konten geschehen. Die von dem System herausfiltrierten Transaktionen müssen schliesslich manuell auf ihre Plausibilität hin überprüft werden. Auch hier verfolgt die Verordnung einen am Risiko des einzelnen Finanzintermediärs orientierten Ansatz. Jeder Finanzintermediär hat grundsätzlich selbst die für ihn sinnvollen Parameter für seine Transaktionsüberwachung zu ermitteln. Die in der Geldwäschereiverordnung

⁶⁹ Vgl. Customer Due Diligence, Fussnote 54, Rz. 10–15.

⁷⁰ Im Wesentlichen werden auf dem Markt drei Typen von Informatikmodellen zur Aufdeckung von verdächtigen Transaktionen angeboten: Die Systeme, die sich darauf beschränken, die Transaktionen nach fixen vorgegebenen Kriterien zu filtern («business rules approach»), diejenigen, die sich auf gegebene Statistiken stützen, um verschiedene Segmente von Risiken innerhalb einer Struktur festzulegen («statistical profiling») und zum Schluss diejenigen, die sich künstlicher Intelligenz bedienen. Die am weitesten entwickelten Systeme sind jene, die die verschiedenen Techniken verbinden.

genannten möglichen Anforderungen sind mithin kein von allen Finanzintermediären einzuhaltender Mindeststandard.⁷¹

Die EBK ist der Auffassung, dass mit dem Einsatz von Informationstechnologie eine effizientere Transaktionsüberwachung möglich ist, und verlangt daher grundsätzlich die Einführung eines geeigneten informatikgestützten Systems. Bei kleineren Verhältnissen soll unter gewissen Voraussetzungen eine manuelle Überwachung möglich sein.

5.6 E-Banking

Die EBK ist grundsätzlich der Auffassung, dass das Internet die Beziehungen zwischen Bank und Kunde nicht fundamental ändert und es sich bei der vollständigen elektronischen Eröffnung von Konten lediglich um eine Unterart einer «non face to face»-Beziehung handelt. Grundsätzlich sind die Risiken dieselben, ob die Transaktion über das Internet abgewickelt wird oder über traditionelle Kanäle. Die Vorschriften zum Umgang mit Geschäftsbeziehungen und Transaktionen mit erhöhten Risiken und insbesondere das Erfordernis einer informatikgestützten Transaktionsüberwachung erweisen sich aus Sicht der EBK auch für Internet-Banken als adäquat, weshalb keine Sonderregeln erforderlich sind. Die von der EBK am 29. März 2001 verabschiedeten «Mindeststandards für reine Internet-Banken und -Effekthändler» erklären eine persönliche Vorsprache von wichtigen Kunden bei der Kontoeröffnung für obligatorisch. Ebenfalls wird bei Sitzgesellschaften eine persönliche Vorsprache des wirtschaftlich Berechtigten verlangt, und zwar nach denselben Kriterien wie für die Kontoeröffnung bei natürlichen Personen. Die Verordnung erklärt den fehlenden Kontakt zur Vertragspartei oder zum wirtschaftlich Berechtigten zu einem weiteren Kriterium für die Qualifikation einer Geschäftsbeziehung als mit höheren Risiken behaftet. Das durch mangelnden direkten Kundenkontakt bedingte potentiell höhere Risiko soll insbesondere bei reinen Internet-Banken im Rahmen der Bildung

⁷¹ Das System muss aber jedenfalls in der Lage sein, Bartransaktionen in der Höhe von über 100 000 Franken zu ermitteln, Art. 8 Abs. 3 Bst. a und Art. 12 Abs. 1 GwV-EBK.

von Risikokategorien sowie durch die Transaktionsüberwachung und die Ansetzung niedrigerer Schwellenwerte kompensiert werden. Nach Ansicht der EBK trägt die Verordnung den wesentlichen Anliegen der Mindeststandards Rechnung.

5.7 Globale Überwachung von Reputationsrisiken

Rechts- und Reputationsrisiken wie auch die anderen Risiken des Bankengeschäfts kennen keine Landesgrenzen. Die Geldwäschereiprävention ist nur wirksam, wenn sie auf konzernweiter Basis funktioniert. Die Erfassung, Begrenzung und Überwachung der von einzelnen Geschäftsbeziehungen ausgehenden Rechts- und Reputationsrisiken kann nur auf konsolidierter Basis wirksam durchgeführt werden. Die Geldwäschereirichtlinien der EBK verbieten es den Finanzintermediären, zur Umgehung dieser Richtlinien ihre ausländischen Zweigniederlassungen oder andere Gruppengesellschaften im Ausland, die im Banken- oder Finanzbereich tätig sind, einzusetzen.⁷² Die Verordnung präzisiert dieses Verbot, indem sie eine Anwendung der grundlegenden Prinzipien der Verordnung auf Zweigniederlassungen und Gruppengesellschaften des Finanzintermediärs im Ausland vorsieht.

Zudem werden internationale Finanzgruppen, die ihren Sitz in der Schweiz haben, verpflichtet, Rechts- und Reputationsrisiken aufgrund von Geldwäscherei oder Terrorismusfinanzierung global zu erfassen, zu begrenzen und zu überwachen. Zu diesem Zweck müssen das interne Überwachungsorgan sowie die externe Revisionsstelle der Gruppe Zugang zu Informationen über die Vertragsparteien sowie die wirtschaftlich Berechtigten von Geschäftsbeziehungen der Gruppengesellschaften haben. Für Schweizer Finanzgruppen nicht erforderlich und für ausländische Finanzgruppen mit schweizerischen Tochtergesellschaften in Bezug auf deren Kunden nicht zulässig sind aber zentrale Kundendatenbanken. Finanzintermediäre mit Sitz in der Schweiz, die Teil einer schweizerischen oder internationalen Gruppe

⁷² Randziffer 6 EBK-RS 98/1.

sind, haben den Überwachungsorganen der Gruppe den Zugang zu Informationen in Bezug auf ihre Geschäftsbeziehungen zu ermöglichen, soweit diese Informationen für die globale Überwachung von Reputationsrisiken erforderlich sind. Diese neuen Bestimmungen entsprechen den letzten Entwicklungen der internationalen Standards.⁷³

5.8 Kampf gegen die Terrorismusfinanzierung

Im Nachgang zu den Ereignissen des 11. Septembers 2001 erlangte die Bekämpfung der Terrorismusfinanzierung auf internationaler Ebene erste Priorität. Da terroristische Organisationen zur Finanzierung auf die Zahlungsverkehrssysteme der Banken angewiesen sind, sollten die Geldwäschereiregeln verschärft auch zur Bekämpfung der Terrorismusfinanzierung angewendet werden. Die von den Vereinigten Staaten ergriffenen Initiativen zur Fahndung nach Terroristengeldern sowie die Verabschiedung der 8 FATF-Spezialempfehlungen gegen die Terrorismusfinanzierung verstärkten den Druck auf die nationalen Rechtssysteme, die notwendigen gesetzgeberischen und regulatorischen Massnahmen zu ergreifen. Eine entsprechende Erweiterung des Anwendungsbereichs der Verordnung erwies sich daher als zwingend.

6 Sorgfaltspflichtvereinbarung

Die Identifizierung der Vertragsparteien und die Feststellung der wirtschaftlich Berechtigten durch die Banken ist ein zentrales Element in der Geldwäschereibekämpfung, welche auch in Zukunft durch die Sorgfaltspflichtvereinbarung im Detail geregelt wird.

Die revidierte Sorgfaltspflichtvereinbarung wurde nach erfolgreicher Absprache mit der Bankenkommission vom Verwaltungsrat der Bankiervereinigung am 2. Dezember 2002 verabschiedet. Die von der Arbeitsgruppe KYC erstellten Prüfungspunkte⁷⁴ für die Revision der

⁷³ Vgl. Customer Due Diligence, Fussnote 54, Rz. 63 ff.

⁷⁴ Siehe Bericht der Arbeitsgruppe KYC, Anhang II (Fussnote 1).

Sorgfaltspflichtvereinbarung wurden weitgehend berücksichtigt. Das Inkrafttreten der Vereinbarung wurde auf den 1. Juli 2003 festgelegt und wird somit zeitgleich mit dem Inkrafttreten der Verordnung erfolgen.

Einige wesentliche Änderungen gegenüber der VSB aus dem Jahre 1998 sind die folgenden⁷⁵:

- Die Präambel ergänzt die Zielsetzung der VSB um die Bekämpfung der Terrorismusfinanzierung.
- Es wird ausdrücklich erwähnt, dass die besonderen Abklärungspflichten bei ungewöhnlichen Geschäftsbeziehungen durch die Geldwäschereiverordnung der EBK geregelt werden (und deshalb auch nicht als Verletzung der VSB durch die Aufsichtskommission sanktioniert werden können).
- Die Identifizierungsart «persönlich bekannt» wird aufgegeben. Es werden nur noch amtliche Ausweispapiere mit Fotografie anerkannt.
- Die Postzustellung zu Identifizierungszwecken wird aufgegeben. Jedoch wird sie zur Überprüfung der Adresse beibehalten.
- Die Ausnahmeregelung für Minderjährigenkonten wird aufgegeben. Es wird die Identifizierung des Erwachsenen verlangt, der das Konto für den Minderjährigen eröffnet.
- Die VSB gewährt nunmehr in Ausnahmefällen eine 30-tägige Nachfrist zur Ergänzung von unvollständigen Kontoeröffnungsunterlagen. Rückzüge auf Verlangen des Kunden sind während dieser Frist nicht möglich.
- Die VSB enthält eine neue Regelung zur Delegation der Identifizierung, welche mit der Regelung der Verordnung zur Delegation der zusätzlichen Abklärungen übereinstimmt. Demnach darf die Bank die Identifizierung mittels einer schriftlichen Vereinbarung an Personen oder Unternehmen delegieren, wenn sie diese über ihre Aufgaben instruiert hat und sie kontrollieren kann, ob die Identifizierung

⁷⁵ Weitere Hinweise zu den Neuerungen der VSB finden Sie auf der Website der SBVg <http://www.sba.ch>.

richtig durchgeführt wird. Der Beauftragte hat die Identifizierungsakten an die Bank zu übermitteln. Eine Weiterdelegation durch den Beauftragten ist ausgeschlossen.

- Die für das Formular A als zwingend bezeichneten Angaben wurden um das Geburtsdatum und die Nationalität des wirtschaftlich Berechtigten erweitert.
- Die Regelung verdeutlicht, dass regelmässig Überlegungen darüber anzustellen sind, ob der Vertragspartner auch der wirtschaftlich Berechtigte ist.
- Zusätzliche Sorgfaltspflichten gelten bei «charities», namentlich Vereinen und Stiftungen. Die Banken haben zusätzlich die eröffnenden Personen zu identifizieren, sofern diese zeichnungsberechtigt sind.
- Die Wohltätigkeitsorganisationen sind nicht mehr grundsätzlich von der Pflicht befreit, den wirtschaftlich Berechtigten festzustellen. Es handelt sich dabei um eine Umsetzung der speziellen Empfehlungen der FATF betreffend die Terrorismusfinanzierung. Das auf dem Korrespondenzweg durchgeführte Kontoeröffnungsverfahren, das von nun an auch auf reine Internetinstitute anwendbar ist, wurde präzisiert.
- Wird die Geschäftsbeziehung auf dem Korrespondenzweg oder über Internet aufgenommen, so prüft die Bank die Identität des Vertragspartners, indem sie sich eine echtheitsbestätigte Kopie eines Identifikationsdokuments zustellen und zudem die Wohnsitzadresse des Vertragspartners durch Postzustellung oder auf andere, gleichwertige Weise bestätigen lässt.
- Banken aus Ländern ohne angemessene Aufsicht und Regelung in Bezug auf die Bekämpfung der Geldwäscherei haben die wirtschaftlich Berechtigten bekannt zu geben, wenn sie für ungenannte Kunden rubrizierte Unterkonti bei einer Schweizer Bank führen. Wenn von im Ausland domizilierten Banken und anderen Finanzintermediären die Rede ist, «die einer angemessenen Aufsicht und Regelung in Bezug auf die Bekämpfung der Geldwäscherei unterstehen», ver-

steht die VSB darunter die Länder, die der Financial Action Task Force on Money Laundering (FATF) angeschlossen sind.⁷⁶

7 Kommentar zur Verordnung

7.1 Allgemeine Bestimmungen

Art. 1 Begriffe

Die Umschreibung der *politisch exponierten Personen (PEP)* wurde offen formuliert mit der Überlegung, dass die Bedeutung einer Funktion vom einen zum anderen Land stark variieren kann (Bst. a). Wie bisher sollen Schweizer PEP, d.h. Personen mit öffentlichen Funktionen in der Schweiz, nicht von der Regulierung erfasst werden.⁷⁷ Die gegen-
teilige Lösung hätte den Kreis der betroffenen Personen stark ver-
grössert, was zu praktischen Schwierigkeiten geführt hätte, wenn die
Geschäftsleitungen der Banken über solche Geschäftsbeziehungen
entscheiden müssten. Werden Geschäftsbeziehungen mit Schweizer
PEP nicht wie solche mit ausländischen PEP ex lege als erhöhtes Ri-
siko betrachtet, schliesst dies nicht aus, dass sie im Einzelfall von ei-
ner Bank aufgrund der von ihr entwickelten Risikokriterien (Art. 7
Abs. 2) oder der Transaktionsüberwachung als solches angesehen wer-
den müssen. In diesem Fall gelten die genau gleichen Abklärungs-
pflichten wie bei ausländischen PEP. Eine PEP, welche ihre öffentliche
Funktion aufgibt, soll ihren Status als PEP *nicht* auf unbegrenzte Zeit
behalten, sofern sie nicht zum Beispiel weiterhin einer anderen PEP
nahe steht.

Die Verordnung integriert soweit nötig die heute in den Richtlinien für
die Reglementierung des professionellen Notenhandels in den Ban-

⁷⁶ Siehe die Liste der FATF-Mitglieder in Fussnote 41. Die im Fürstentum Liechtenstein domizilierten Banken und anderen Finanzintermediäre werden den entsprechenden Finanzintermediären aus den FATF-Ländern gleichgestellt.

⁷⁷ Ebenso bisher die Geldwäschereichtlinien der EBK und nun die Regelung in den USA, vgl. Proposed Rules vom US Treasury S. 10 und 27 (Umsetzung des § 312 des Patriot Act), erhältlich über Internet: <http://www.treas.gov/press/releases/docs/nprm.pdf>.

ken⁷⁸ enthaltenen Bestimmungen. Die Definition des professionellen Notenhändlers (Bst. b) entspricht inhaltlich weitgehend der bisherigen, wurde aber gekürzt.

Da die zur Umsetzung der Terrorismusfinanzierungskonvention notwendigen Änderungen des Strafgesetzbuches noch hängig sind, fehlt es im geltenden Recht an einer Definition des Terrorismus sowie der Terrorismusfinanzierung, auf welche verwiesen werden könnte. Die EBK kommt indes nicht umhin, zur Präzisierung der Pflichten der Finanzintermediäre und Umsetzung der internationalen Empfehlungen⁷⁹ den Begriff der terroristischen Organisation sowie der Terrorismusfinanzierung zu verwenden (Bst. c). Als terroristische Organisation sollen daher kriminelle Organisationen im Sinne von Art. 260^{ter} des Strafgesetzbuches gelten. Gemäss Botschaft war der Tatbestand der Kriminellen Organisation von Artikel 260^{ter} StGB von Anfang an nicht nur auf mafiose, sondern auch auf terroristische Organisationen zugeschnitten.⁸⁰ Es wird sich allenfalls als notwendig erweisen, die Definition bei Abschluss der derzeit noch hängigen Strafrechtsreform anzupassen.

Art. 2 Geltungsbereich

Die Verordnung sieht gegenüber den geltenden Geldwäschereirichtlinien keine grundsätzlichen Änderungen in Bezug auf den Anwendungsbereich vor (Absatz 1).

Artikel 2 übernimmt die in Absprache mit der Kontrollstelle bereits in Randziffer 5 der Geldwäschereirichtlinien erwähnte Möglichkeit, auch schweizerische Gruppengesellschaften von Banken oder Effektenhändlern der Geldwäschereiüberwachung der EBK zu unterstellen, die keiner spezialgesetzlichen Aufsicht unterstellt sind⁸¹, jedoch Aktivitäten im Finanzbereich gemäss Art. 2 Abs. 3 des Geldwäschereigesetzes

⁷⁸ <http://www.ebk.admin.ch/f/publik/bulletin/bull20.pdf>; S. 101 (nur in deutscher Fassung).

⁷⁹ Siehe vorne Ziff. 4.2 und 4.3.

⁸⁰ Vgl. Botschaft des Bundesrates vom 30. Juni 1993, BBl 1993 III 277 ff. (296).

⁸¹ Entsprechend Art. 2 Abs. 2 GwG.

ausüben. Diese Möglichkeit wird aber nur auf Gesuch hin gewährt. Zudem müssen die Voraussetzungen der Buchstaben a bis e erfüllt sein. Die Unterstellungsmöglichkeit gilt auch für Schwestergesellschaften von Banken und Effektenhändlern. Ziel dieser Unterstellungsmöglichkeit ist es, das von der Verordnung geforderte gruppenweite Management der Reputations- und Rechtsrisiken nach einheitlichen Standards (Art. 9) bei inländischen Gesellschaften auch aufsichtsrechtlich zu überwachen.

Durch die in Absatz 2 festgelegten Bedingungen soll die Gleichbehandlung zwischen den Finanzintermediären, welche der vorliegenden speziellen Bestimmung unterworfen sind, und denjenigen, welche eine identische Tätigkeit ausüben, jedoch der Überwachung durch die Kontrollstelle unterworfen sind, sichergestellt werden. Da die antragstellende Gesellschaft nicht der umfassenden Aufsicht durch die EBK unterstellt ist, muss sie die Aufsichtshoheit der EBK anerkennen (Abs. 2 Bst. c). Zudem muss auch die Gruppe, welche selbst der konsolidierten Aufsicht der EBK unterstellt ist, für die Einhaltung der Verordnung bei den Gruppengesellschaften sorgen, welche sie der EBK-Aufsicht unterstellen will (Abs. 2 Bst. d). Dies entspricht der Pflicht zur gruppenweiten Überwachung der Reputations- und Rechtsrisiken.⁸²

Der externe Revisor der Gruppe muss eine Kontrolle für jede Gruppengesellschaft vornehmen, die Artikel 2 Abs. 2 unterliegt. Er muss in seinem Bericht zur Einhaltung des Geldwäschereigesetzes und der Verordnung, aber auch der Sorgfaltspflichtvereinbarung (Art. 14 Abs. 1), für jede einbezogene Gruppengesellschaft einzeln Stellung nehmen (Art. 31).

Art. 3 Ausländische Zweigniederlassungen und Gruppengesellschaften

Diese Bestimmung geht etwas weiter als die Geldwäschereirichtlinien, die nur die Verwendung von ausländischen Zweigniederlassungen oder Gruppengesellschaften im Ausland zum Zwecke der Umgehung

⁸² Siehe Art. 9 hiernach.

der Richtlinien verbieten.⁸³ In Übereinstimmung mit den Empfehlungen des Customer Due Diligence Paper⁸⁴ sind die grundlegenden Prinzipien der Verordnung auch auf ausländische Zweigniederlassungen und ausländische Gesellschaften schweizerischer Gruppen anwendbar. Erfasst sind die im Finanzbereich tätigen und nach den Eigenmittelvorschriften konsolidierungspflichtigen (Art. 1 Bst. d) Tochter- und allenfalls auch Schwestergesellschaften.

Erwächst einem Finanzintermediär jedoch aus der Anwendung der Grundsätze der Verordnung ein Wettbewerbsnachteil gegenüber seinen lokalen Konkurrenten, soll er die EBK informieren, ebenso, wenn lokale Vorschriften die Anwendung der Verordnung verbieten (Absatz 2). Diese wird die Situation beurteilen und im Kontakt mit den lokalen Behörden die Situation zu klären versuchen. Gelingt dies nicht, stehen der EBK je nach Umständen verschiedene Optionen offen: so im Extremfall das Verbot, in dieser Jurisdiktion eine Niederlassung zu unterhalten oder umgekehrt die Befreiung der Gruppe von der Einhaltung einzelner Grundsätze der Verordnung. Für die Meldung von verdächtigen Transaktionen oder Beziehungen und die Blockierung von Vermögenswerten gelten aber in jedem Fall nur die lokalen Bestimmungen (Absatz 3).

7.2 Grundsätze

Art. 4 Verbot der Annahme von Vermögenswerten aus Korruption und anderen Verbrechen

Die vorsätzliche Entgegennahme⁸⁵ von Vermögenswerten krimineller Herkunft ist Geldwäscherei im Sinne von Art. 305^{bis} des Strafgesetzbuches, da sie eine potentielle Vereitelung der Ermittlung der Herkunft, der Auffindung oder der Beschlagnahme von Vermögenswerten darstellt (Absatz 1). Als Verbrechen gelten alle Taten, welche das

⁸³ Siehe Randziffer 6 EBK-RS 98/1.

⁸⁴ Vgl. Customer Due Diligence, Fussnote 54; siehe auch Ziff. 4.5 hiervor.

⁸⁵ Für die Definition von Vorsatz siehe Art. 18 Abs. 2 StGB.

Schweizer Recht mit Zuchthaus bedroht⁸⁶, und zwar grundsätzlich auch solche, die im Ausland begangen wurden.⁸⁷ Vortat zu Geldwäscherei soll auch die gewerbmässige Geldwäscherei grosser Summen sein.⁸⁸

Absatz 2 nennt speziell einige Verbrechen im Zusammenhang mit der Korruption und dem Missbrauch öffentlicher Gelder. Diese besondere Erwähnung wäre rechtlich nicht notwendig. Sie schadet aber nicht, weil sich gerade die Annahme solcher Gelder als eines der grössten Reputationsrisiken für die Banken und den Finanzplatz erwiesen haben, wie die Fälle Abacha und Montesinos zeigten.

Die fahrlässige Entgegennahme von Vermögenswerten, die aus einem Verbrechen stammen, ist strafrechtlich nicht relevant. Finanzintermediäre, die der Aufsicht der EBK unterstellt sind, dürfen ihre Tätigkeit jedoch erst nach Erteilung einer Bewilligung ausüben.⁸⁹ Deren Erteilung (und Aufrechterhaltung) hängt von der Erfüllung gewisser Voraussetzungen ab, darunter der Gewähr für eine einwandfreie Geschäftstätigkeit.⁹⁰ Nimmt ein Finanzintermediär fahrlässig Vermögenswerte entgegen, die aus einem Verbrechen stammen, kann fraglich sein, ob diese Bewilligungsvoraussetzung noch erfüllt ist (Absatz 3).

Art. 5 Verbot von Geschäftsbeziehungen mit kriminellen und terroristischen Organisationen

Geldwäscherei bildet auch die Entgegennahme von Vermögenswerten krimineller oder terroristischer Organisationen. Ein Angestellter⁹¹ ei-

⁸⁶ Art. 9 und 35 StGB.

⁸⁷ Art. 305^{ter} Ziff. 3 StGB.

⁸⁸ Art. 305^{ter} Ziff. 2 Bst. c StGB.

⁸⁹ Für Banken: Art. 3 ff. BankG; für Börsen: Art. 3 BEHG; für Effektenhändler: Art. 10 BEHG; für Anlagefondslösungen: Art. 10 AFG.

⁹⁰ Für die Definition der Gewähr einer einwandfreien Geschäftstätigkeit in diesem Zusammenhang siehe EBK-Bulletin 40/2000, S. 24 (<http://www.ebk.admin.ch/f/publik/bulletin/bull40.pdf>).

⁹¹ Nach dem neuen Unternehmensstrafrecht (Art. 102 und Art. 102a neuStGB) soll in Zukunft bei diesen Delikten grundsätzlich auch das Unternehmen strafbar sein, wenn es nicht alle erforderlichen und zumutbaren Vorkehrungen zur Verhinderung solcher Taten getroffen hat.

nes Finanzintermediärs, der dies vorsätzlich tut, kann sich sogar der Unterstützung einer kriminellen Organisation strafbar machen.

Art. 6 Korrespondenzbankbeziehungen

Die Regeln der Verordnung gelten auch für Korrespondenzbankbeziehungen (Abs. 1), d.h. auch Korrespondenzbankbeziehungen können erhöhte Risiken beinhalten. Entsprechend den internationalen Vorgaben dürfen die Finanzintermediäre in Zukunft keine Geschäftsbeziehungen mit Banken unterhalten, die keine physische Präsenz an ihrem Inkorporationsort haben («shell banks»), das heisst nicht dauernd Personal beschäftigen. Ausgenommen sind Geschäftsbankbeziehungen mit Banken, die Teil einer unter umfassender Aufsicht stehenden Finanzgruppe sind. Abgesehen von dieser Ausnahme sind Geschäftsbeziehungen mit «shell banks» nicht erlaubt (Abs. 2).

7.3 Organisatorische Massnahmen

Art. 7 Geschäftsbeziehungen mit erhöhten Risiken

Der Grad der anzuwendenden Sorgfalt soll bei Geschäftsbeziehungen höher sein, wenn diese ein erhöhtes Risikopotential aufweisen. Bevor ermittelt werden kann, welche Geschäftsbeziehungen erhöhte Risiken beinhalten, muss jeder Finanzintermediär Risikokriterien entwickeln, welche auf seine besondere Geschäftstätigkeit zugeschnitten sind (Abs. 4). So sind die Risiken im Private Banking für ausländische Privatkunden nicht die gleichen wie diejenigen einer Bank, welche ausschliesslich im Schweizer Retailgeschäft tätig ist. Im Prinzip genügt es, die Geschäftsbeziehungen in zwei Kategorien einzuteilen, in die normalen und diejenigen mit erhöhtem Risiko. Geschäftsbeziehungen mit erhöhtem Risiko sind nicht unerwünscht oder gar unzulässig. Sie bedürfen aber zusätzlicher Abklärungen (Art. 17). Die Kennzeichnung einer Geschäftsbeziehung als solche mit erhöhtem Risiko sollte in der Regel auf der Basis von Informationen erfolgen können, die bei der Eröffnung des Kontos ohne grosse Nachforschungen verfügbar sind.

Die zu entwickelnden Kriterien müssen unter dem Blickwinkel der rechtlichen Risiken und der Reputationsrisiken sachdienlich sein (Abs. 1). Sie können sich sowohl auf die Vertragspartei als auch auf den wirtschaftlich Berechtigten beziehen. Die Beurteilung, ob eine Geschäftsbeziehung ein erhöhtes Risiko aufweist, soll grundsätzlich zu Beginn der Geschäftsbeziehung⁹² vorgenommen werden, selbst wenn gewisse Informationen erst im Laufe der Beziehung überprüfbar sind.

Absatz 2 enthält eine nicht abschliessende Aufzählung von Kriterien, die verwendet werden können. Gegebenenfalls müssen einige von ihnen gemeinsam angewendet werden, um eine Geschäftsbeziehung als Risikobeziehung einstufen zu können. Einige beziehen sich auf Risikoländer (Bst. a, b und g). Aus politischen und praktischen Gründen wird die EBK keine Listen führen, sondern allenfalls gestützt auf Arbeiten in internationalen Foren wie der FATF den Finanzintermediären Hinweise geben. Auch wenn der persönliche Kontakt zum Kunden (Bst. c) kein Allerweltsmittel ist, trägt er doch zu einer besseren Kenntnis der Person und des sozialen und geschäftlichen Hintergrundes des Kunden bei. Überdies wäre der Versuch eines Kunden, die Abklärungen des Finanzintermediärs zu behindern, verdächtig (Anhang A8). Die Art der gewünschten Leistungen oder Produkte (z.B. Nummernkonti, «back-to-back»-Geschäfte, Treuhandkredite) kann je nach den Umständen und Art der Geschäftstätigkeit des Finanzintermediärs Anlass zu einem erhöhten Risiko bilden (Bst. d). Auch die Höhe der eingebrachten Vermögenswerte kann ein Risikofaktor sein (Bst. e). Die Höhe der Zu- und Abflüsse von Vermögenswerten (Bst. f) muss auf der Basis der Gesamtheit der Aktivitäten des Vertragspartners und/oder des wirtschaftlich Berechtigten beurteilt werden.

Aufgrund der Erfahrungen aus der Vergangenheit gelten Geschäftsbeziehungen mit PEP in jedem Fall als solche mit erhöhtem Risiko (Abs. 3).

⁹² Vgl. Art. 20.

Art. 8 Transaktionen mit erhöhten Risiken

Das dargelegte System für Geschäftsbeziehungen mit erhöhtem Risiko soll mutatis mutandis auch für Transaktionen mit erhöhten Risiken gelten. Wie bereits erwähnt sind die genannten möglichen Anforderungen keine von allen Finanzintermediären einzuhaltenden Mindeststandards, sondern zeigen grundsätzlich mögliche Spezifikationen des Überwachungssystems auf.

Immerhin sollte die Festsetzung eines bestimmten Betrages (Bst. a), über welchem die Transaktionen als solche mit erhöhtem Risiko qualifiziert werden müssen, bei allen Banken möglich sein. Je nach Geschäftstätigkeit sinnvoll und machbar kann auch die Überprüfung erheblicher Abweichungen im Vergleich zur üblichen Verhaltensweise des Klienten sein (Bst. b). Schliesslich kann es je nach Zusammensetzung des Kundenkreises eines Finanzintermediärs und des Transaktionsvolumens angesichts des heutigen technischen Entwicklungsstandes vernünftig sein, ein Transaktionsüberwachungssystem zu betreiben, das Abweichungen der Transaktionen eines einzelnen Kunden von denjenigen einer vergleichbaren Kundengruppe feststellt (Bst. c). Dazu ist allerdings erforderlich, dass sich sinnvoll Kundengruppen definieren lassen, was jedenfalls eine grosse Zahl vergleichbarer Geschäftsbeziehungen voraussetzt und selbst dann nicht für alle Finanzintermediäre Sinn machen kann. Die Finanzintermediäre müssen selbst aufgrund einer Analyse ihrer Risiken und der Struktur ihrer Geschäftsbeziehungen festlegen, welche Art von Transaktionsüberwachung sinnvoll ist. Sofern die zugrunde liegende Risikoanalyse nachvollziehbar ist, wird die EBK ihr Ermessen nicht an die Stelle desjenigen der Finanzintermediäre setzen.

Art. 9 Globale Überwachung der Rechts- und Reputationsrisiken

Finanzintermediäre mit Zweigniederlassungen oder Gruppengesellschaften im Ausland müssen ihre Reputationsrisiken global erfassen, begrenzen und überwachen. Die mit einem Geldwäschereifall oder

dem Auffinden von Terroristengeldern verbundenen rechtlichen Risiken sowie potentiell rufschädigenden Medienberichte können über nationale Grenzen hinaus Auswirkungen auf alle miteinander verbundenen rechtlichen Einheiten haben. Es muss daher die Möglichkeit bestehen, konsolidiert und konzernweit Geschäftsbeziehungen mit Kunden mit erhöhten Risiken zu erfassen und zu überwachen, selbst wenn die Geschäftsbeziehung mit einer ausländischen Zweigniederlassung oder Gruppengesellschaft eingegangen wurde (Absatz 1).

Bei Finanzgruppen muss zu diesem Zweck namentlich eine Compliance-Funktion auf Gruppenebene vorhanden sein, welche im Bedarfsfall Zugang zu Informationen über Vertragsparteien und wirtschaftlich Berechtigte in allen Gesellschaften der Finanzgruppen hat. Im Bedarfsfall muss es möglich sein, konzernweit die Portfolios von allen rechtlichen Einheiten oder Business Units auf bestimmte Geschäftsbeziehungen überprüfen zu lassen. Diese Bestimmung steht im Einklang mit der internationalen Aufsichtspraxis, wonach ein konzernweites zentralisiertes Risikomanagementsystem unter der Verantwortung eines Group Compliance Officer zur globalen Überwachung von Reputationsrisiken generell als erforderlich anerkannt wird.⁹³ Zur Umsetzung dieses Erfordernisses bestehen auf internationaler Ebene verschiedene Praktiken. Die Verordnung verlangt keine zentralen Datenbanken, sondern lediglich einen Zugang zu Kundendaten bei ausländischen Unternehmen im Bedarfsfall, was den internationalen

⁹³ Das Customer Due Diligence Paper des Basler Ausschusses, siehe Ziff. 4.5, verlangt unter Ziffer 16 eine konsolidierte Überwachung von wichtigen Kundenbeziehungen («Oft haben Kunden mehrere Konten bei derselben Bank, aber bei Niederlassungen in verschiedenen Ländern. Um das Reputations-, Compliance- und Rechtsrisiko im Zusammenhang mit solchen Konten wirksam handhaben zu können, sollte eine Bank in der Lage sein, erhebliche Guthaben und Vorgänge auf diesen Konten auf weltweit konsolidierter Basis zusammenzufassen und zu überwachen, unabhängig davon, ob es sich um ein Konto in der Bilanz, ein Konto ausserhalb der Bilanz, Vermögenswerte mit Verwaltungsauftrag oder ein Treuhandkonto handelt.»). Im Nachgang zu den Ereignissen vom 11. September 2001 wurde dieser Gedanke weiterentwickelt und das Vorhandensein eines zentralisierten Risikomanagementsystems zur globalen Überwachung von Reputationsrisiken von Finanzgruppen für erforderlich betrachtet. Siehe Basel Committee Publications No. 89 April 2002 Summary of a meeting of representatives of Supervisors and Legal Experts of G10 Central Banks and Supervisory Authorities on 14 December 2001, Basel, Switzerland, verfügbar auf dem Internet unter <http://www.bis.org/pub/bcbs89.pdf>.

Vorgaben entspricht.⁹⁴ Die Verordnung sieht zudem vor, dass Gruppengesellschaften im Ausland unverzüglich den zuständigen Organen am Hauptsitz in der Schweiz die grundlegenden Informationen zur Gewährleistung einer globalen Überwachung der Rechts- und Reputationsrisiken liefern. Ein solcher Fall liegt beispielsweise vor bei Hinweisen auf Verbindungen eines Kunden zu terroristischen Organisationen. Diese Bestimmungen, welche sich explizit auf Gruppengesellschaften beziehen, sind ad maiore minus auch auf Beziehungen innerhalb derselben juristischen Person anwendbar, so beispielsweise zwischen der Zweigniederlassung und dem Hauptsitz der Gesellschaft (Absatz 2).

Ist der direkte Zugang der zuständigen Organe der Gruppe zu Informationen bei ausländischen Niederlassungen auf Grund restriktiver Bestimmungen des ausländischen Rechts ausgeschlossen, ist die EBK zu informieren. Sie wird im Einzelfall zusammen mit dem Finanzintermediär und allenfalls im Kontakt mit der ausländischen Aufsichtsbehörde eine Lösung suchen müssen. Als letztes Mittel könnte die EBK die Errichtung von Niederlassungen schweizerischer Finanzintermediäre in bestimmten Ländern beschränken oder untersagen (Absatz 3).

Schweizerische Niederlassungen, welche in den Konsolidierungskreis eines ausländischen Finanzintermediärs oder einer ausländischen Finanzgruppe eingeschlossen sind, müssen den Kontrollorganen der ausländischen Mutter Zugang zu Informationen über einzelne Kunden und wirtschaftlich Berechtigte gewähren, sofern diese für die konsolidierte Überwachung der Reputationsrisiken notwendig sind. Auch hier nicht notwendig (und nicht zulässig) sind zentrale Kundendatenbanken, welche Angaben über Kunden schweizerischer Tochterbanken umfassen. Besteht im Einzelfall aber ein Bedürfnis, muss den Organen der ausländischen Mutterbank ein solcher Zugang möglich sein, da ihnen nicht verwehrt werden kann, was für die Kontrollorgane schwei-

⁹⁴ Siehe auch Sharing of financial records between jurisdictions in connection with the fight against terrorist financing, Fussnote 55.

zerischer Finanzintermediäre bei ausländischen Niederlassungen im Rahmen eines globalen Risikomanagements als notwendig erachtet wird (Absatz 4).

Art. 10 Interne Geldwäschereiweisungen

Die Verordnung verlangt wie die geltenden Richtlinien der EBK⁹⁵ interne Weisungen zur Bekämpfung der Geldwäscherei. Sie sind allen betroffenen Mitarbeiterinnen und Mitarbeitern mitzuteilen. Nicht zwingend ist es, die Weisungen in einem einzigen Erlass zusammenzufassen. Je nach der Organisation des Weisungswesens eines Finanzintermediärs können andere Wege sinnvoller sein.

Absatz 2 regelt den Minimalinhalt der Weisungen. Die Buchstaben a) – d) und i) enthalten im Vergleich zu den Geldwäschereirichtlinien neue Aufgaben. Was den Masstab anbelangt, den der Finanzintermediär anwenden sollte, um die erhöhten Risiken zu erfassen, zu begrenzen und zu überwachen (Bst. c), müssen Verfahren und Verantwortlichkeiten für die zusätzlichen Abklärungen bei Geschäftsbeziehungen mit erhöhten Risiken festgelegt werden.

Die Bedeutung der Thematik rechtfertigt es, dass die Weisungen durch die Geschäftsleitung oder bei kleineren Finanzintermediären durch den Verwaltungsrat erlassen werden (Absatz 3).

Art. 11 Ausbildung des Personals

Die Mitarbeiterinnen und Mitarbeiter eines Finanzintermediärs müssen bei Antritt ihrer Stelle eine ihren Aufgaben entsprechende Ausbildung auf dem Gebiet der Geldwäscherei erhalten. Diese Ausbildung muss für alle Mitarbeiterinnen und Mitarbeiter, die von der Geldwäschereibekämpfung betroffen sind, regelmässig wiederholt und auf den neusten Stand gebracht werden.

⁹⁵ Vgl. Ziff. 15 EBK-RS 98/1.

Art. 12 Systeme zur Transaktionsüberwachung

Artikel 6 des Geldwäschereigesetzes verlangt von den Finanzintermediären, die wirtschaftlichen Hintergründe und den Zweck ungewöhnlicher Transaktionen abzuklären, wenn ihre Rechtmässigkeit nicht erkennbar ist. Dazu ist in einem ersten Schritt aber die ungewöhnliche Transaktion als solche zu erkennen. Finanzintermediäre sollen in Zukunft, soweit sie dies nicht bereits tun, ein informatikgestütztes System einsetzen, welches ihnen hilft, Transaktionen mit erhöhten Risiken zu erkennen (Absatz 1). Dabei erlaubt die Verordnung, die Systemanforderungen flexibel der Geschäftstätigkeit der Finanzintermediäre anzupassen.⁹⁶ Die Neueinführung entsprechender Software ist sehr aufwändig, was bei der Festsetzung der Übergangsfrist in der Verordnung dementsprechend berücksichtigt wurde.⁹⁷

Diese Informatiksysteme sind nur (aber immerhin) ein Hilfsmittel. Letztlich müssen die verantwortlichen Mitarbeiterinnen und Mitarbeiter des Finanzintermediärs die vom System generierten Berichte auf ihre Bedeutung prüfen. Transaktionen, welche nicht plausibel sind, sollten genauer abgeklärt werden. Die vom System produzierten Daten müssen nicht quasi zeitgleich mit der Ausführung der Transaktion, aber innerhalb vernünftiger Fristen überprüft werden. Vom Finanzintermediär wird auch nicht verlangt, dass er eine Transaktion vor der Ausführung auf erhöhte Risiken prüft. Schliesslich ist entsprechend der internationalen Praxis auch nicht erforderlich, dass der gesamte Zahlungsverkehr auf «verdächtige» Auftraggeber oder Zahlungsempfänger geprüft wird (Absatz 2).

In kleinen Verhältnissen kann sich eine informatikgestützte Transaktionsüberwachung als zu aufwändig und daher als unverhältnismässig und nicht notwendig erweisen. In diesem Fall kann der Finanzintermediär auf die Einsetzung eines informatikgestützten Systems verzichten, ohne jedoch von der Pflicht befreit zu werden, die Transaktionen auf andere Art zu überwachen. Die Grenze zur Befreiung von der

⁹⁶ Vgl. vorne Anmerkungen zu Art. 8.

⁹⁷ Vgl. hinten Anmerkungen zu Art. 32.

informatikgestützten Transaktionsüberwachung kann nicht abstrakt festgelegt werden. Grundsätzlich ist jeder Finanzintermediär frei, auf ein solches System zu verzichten, sofern er die Transaktionen ebenso wirksam «von Hand» überwachen kann, was allerdings nicht einfach sein dürfte. In diesem Fall muss zudem die Revisionsstelle alljährlich schwerpunktmässig prüfen, ob eine manuelle Überwachung vorhanden ist und funktioniert (Absatz 3).

Art. 13 Interne Geldwäschereifachstelle

Im Allgemeinen wird die interne Geldwäschereifachstelle wahrscheinlich der «Compliance»-Abteilung des Finanzintermediärs zugeordnet sein, sei es generell oder als Teil derselben. Die Geldwäschereifachstelle soll nur beratende und unterstützende Aufgaben erfüllen. Die Verantwortung für die Geschäftsbeziehungen muss bei der Linie bleiben. Dies bedeutet generell, dass Kundenbetreuer nicht davon absehen können, ihren Kunden gegebenenfalls die nötigen Fragen zu stellen.

Die «Compliance»-Abteilung bereitet die internen Weisungen zur Geldwäscherei zu Handen der Direktion vor⁹⁸ (Abs. 2 Bst. a) und überwacht in Absprache mit den internen und externen Revisoren sowie den Linienverantwortlichen deren Vollzug (Abs. 2 Bst. b). Die Verantwortung der Organisation der Geldwäschereiausbildung obliegt ihr (Abs. 2 Bst. c)⁹⁹ ebenso wie die Festsetzung von Parametern zur Überwachung von Transaktionen gemäss Art. 12 (Abs. 2 Bst. d). Die interne Geldwäschereifachstelle nimmt im Prinzip nicht selbst die Überprüfung der Informationen des Transaktionsüberwachungssystems vor, stellt aber sicher, dass die zuständigen Personen der Linie regelmässig und sorgfältig die Relevanz dieser Ergebnisse überprüfen (Abs. 2 Bst. e). In Fällen, in welchen zusätzliche Abklärungen durchgeführt werden müssen, muss die interne Geldwäschereifachstelle entweder selbst tätig werden oder die bei der Linie zuständigen Mitarbeiter damit beauftragen. Sie muss sicherstellen, dass das für den Entscheid

⁹⁸ Art. 10 Abs. 3.

⁹⁹ Art. 11.

über die Aufnahme oder Weiterführung einer Beziehung mit erhöhten Risiken zuständige Organ regelmässig die nötigen Unterlagen erhält, um seinen Entscheid zu fällen (Absatz 2 Bst. g).

Die Möglichkeiten einer Auslagerung der Geldwäschereifachstelle sind relativ grosszügig formuliert. Sie stehen nicht nur Finanzintermediären offen, die auf Grund ihrer Grösse oder Organisation nicht in der Lage sind, eine solche Stelle einzurichten, sondern sind auch in Fällen möglich, in welchen eine solche Einrichtung, beispielsweise aufgrund der Einbettung in eine Gruppenstruktur, unzweckmässig wäre. Im Weiteren sind die generellen Anforderungen an die Auslagerung von Geschäftsbereichen (Outsourcing)¹⁰⁰ anwendbar (Abs. 3).

7.4 Allgemeine Sorgfaltspflichten

Art. 14 Identifizierung der Vertragspartei und Feststellung des wirtschaftlich Berechtigten

Wie bisher gemäss Randziffer 10 der Geldwäschereirichtlinien gelten die Bestimmungen der VSB betreffend die Feststellung der Identität der Vertragsparteien und der wirtschaftlich Berechtigten für alle Finanzintermediäre, die der Geldwäschereiaufsicht der EBK unterstehen (Absatz 1). Entgegen dem Vernehmlassungsentwurf sieht die Verordnung nicht ausdrücklich die Möglichkeit der EBK vor, von der VSB abweichende Bestimmungen zu erlassen. Diese Befugnis ergibt sich jedoch für die EBK direkt aus dem Geldwäschereigesetz.¹⁰¹

Art. 15 Angabe der Auftraggeber bei Zahlungsaufträgen

Diese Bestimmung setzt die Empfehlung VII der Besonderen Empfehlungen der FATF gegen die Terrorismusfinanzierung¹⁰² um, wonach Überweisungen genaue und verständliche Angaben über den Auftraggeber enthalten müssen. Im Februar 2003 verabschiedete die FATF eine Weisung («interpretative note») zur Umsetzung von FATF-Emp-

¹⁰⁰ Siehe EBK-RS 99/2 «Outsourcing».

¹⁰¹ Art. 16 und 41 GwG.

¹⁰² Siehe Kap. 4.2.

fehlung VII.¹⁰³ Gemäss dieser Weisung wird grundsätzlich immer die Angabe des Namens und, sofern ein Konto besteht, auch der Kontonummer des Auftraggebers verlangt. Zusätzlich soll auf Zahlungsaufträgen auch die Adresse des Auftraggebers angegeben werden, wobei diese jedoch entweder durch eine nationale Identitätsnummer, eine Kundenidentifizierungsnummer oder das Geburtsdatum sowie den Geburtsort des Auftraggebers ersetzt werden kann. Eine Ausnahme ist für inländische Überweisungen zulässig, sofern in diesen Fällen ein Zugriff auf die Angaben durch die zuständigen nationalen Behörden gewährleistet ist.

Die vorliegende Bestimmung orientiert sich an den Vorgaben der FATF. Der Finanzintermediär hat demnach grundsätzlich bei allen Zahlungsaufträgen den Namen, die Kontonummer und das Domizil des Auftraggebers anzugeben. In allen Fällen ist die Angabe des Namens des Auftraggebers erforderlich. Die übrigen Angaben können durch eine Identifizierungsnummer ersetzt werden, sofern diese erlaubt, die Transaktion bzw. Kontobeziehung des Auftraggebers, von der die Transaktion ausgeht, festzustellen. In Übereinstimmung mit den Vorgaben der FATF¹⁰⁴ beschränken sich diese Anforderungen auf den grenzüberschreitenden Zahlungsverkehr (Absatz 1). Die Finanzintermediäre können bei Vorliegen berechtigter Gründe von der Angabe gewisser Informationen über den Auftraggeber gemäss Absatz 1 absehen, wenn sie diese Gründe abklären und auf ihre Plausibilität hin überprüfen. Die durchgeführten Abklärungen müssen dokumentiert werden (Absatz 2). Die Angabe des Kundennamens darf nicht ohne Zustimmung des Kunden erfolgen. Dies bedeutet, dass die Bank Inhaber von Nummernkonti vor Ausführung von Zahlungsaufträgen ins Ausland darauf hinweisen muss, dass der Name bei Überweisungen ins Ausland grundsätzlich angegeben werden muss. Bei Zahlungsaufträgen über Namenkonti hingegen wird bereits heute regelmässig –

¹⁰³ Interpretative Note to FATF Special Recommendation VII: Wire Transfers, 13. Februar 2003: http://www.fatf-gafi.org/pdf/INSR7_en.PDF.

¹⁰⁴ Vgl. FN 103.

andere Anweisungen des Kunden vorbehalten – der Name des Kunden angegeben.

Art. 16 Professioneller Notenhandel

Es ist keine Änderung der geltenden Richtlinien der Bankenkommission zum professionellen Notenhandel in den Banken¹⁰⁵ vorgesehen. Ihr Inhalt wird aber gestrafft.

7.5 Erhöhte Sorgfaltspflichten

Art. 17 Zusätzliche Abklärungspflichten bei erhöhten Risiken

Art. 6 GwG sieht eine besondere Abklärungspflicht bei ungewöhnlichen Transaktionen oder Geschäftsbeziehungen vor. Die Verordnung präzisiert, was von den Finanzintermediären diesbezüglich verlangt wird. Bei Geschäftsbeziehungen und bei Transaktionen mit erhöhten Risiken sind systematisch Abklärungen vorzunehmen, die über die Routine-Identifizierung hinausgehen, welche die VSB im Rahmen einer Kontoeröffnung verlangt. Bei den anderen, «normalen» Geschäftsbeziehungen genügen hingegen die Vorgaben der VSB. Das Ziel der zusätzlichen Abklärungen ist es, weitere Informationen über den Kunden und sein Umfeld zu sammeln, die es erlauben, das Risiko der Geschäftsbeziehung genauer beurteilen zu können. Mit den zusätzlichen Angaben dieser Abklärungen entsteht ein Kundenprofil. Es wird aber auf diesen Ausdruck verzichtet, um Verwechslungen mit Abklärungen zu vermeiden, welche ein anderes Ziel haben, beispielsweise die optimale Beratung des Kunden in der Vermögensverwaltung und im Effektenhandel. Selbstverständlich können Informationen derartiger vorhandener «Kundenprofile» auch zur Geldwäschereibekämpfung verwendet werden. In der Regel dürften die zu Beratungszwecken erhobenen Angaben aber den Anforderungen an die zusätzlichen Abklärungen nicht genügen. Dagegen muss hervorgehoben werden, dass die Bestimmungen über den Datenschutz¹⁰⁶ vollumfänglich Anwendung auf die Erhebung und Auswertung dieser Informationen finden.

¹⁰⁵ Siehe bei Art. 1.

¹⁰⁶ Bundesgesetz vom 19. Juni 1992 über den Datenschutz, SR 235.1.

Angeichts der grossen Zahl von Geschäftsbeziehungen wäre es unrealistisch und würde keine sinnvollen Resultate hervorbringen, solche Abklärungen für sämtliche Kunden zu verlangen. Es sollen nicht breitflächige Abklärungen oberflächlich, sondern risikoorientierte gezielte Abklärungen vertieft gemacht werden. Die Abklärungen müssen aber mit vernünftigem Aufwand durchführbar sein (Abs. 1).

Der Absatz 2 enthält eine nicht abschliessende Aufzählung einzelner Fragen (zum Beispiel zur Herkunft der eingebrachten Vermögenswerte und zum Ursprung des Kundenvermögens), welche je nach Umständen bei Geschäftsbeziehungen oder Transaktionen mit erhöhtem Risiko abzuklären sind. Ziel ist, so viele Informationen wie nötig zu sammeln, um eine tragfähige Grundlage für eine Risikobeurteilung zu schaffen. Diese Informationsbeschaffung ist eine Holschuld der Finanzintermediäre. Sie müssen ausreichend abklären und dürfen sich nicht einfach mit unzureichenden Erklärungen des Kunden zufrieden geben, auch wenn dies im Einzelfall heikel sein kann.

Die Finanzintermediäre dürfen Geschäftsbeziehungen mit erhöhten Risiken führen, wenn sie aufgrund der zusätzlichen Abklärungen zum Schluss kommen, dass diese Risiken verantwortbar sind. Geschäftsbeziehungen mit erhöhten Risiken sind nicht per se unerwünschte oder unerlaubte Geschäftsbeziehungen. Dies gilt auch für Geschäftsbeziehungen mit politisch exponierten Personen. Der Finanzintermediär muss seine Risiken aber kennen und beurteilen können.

Art. 18 Abklärungsmittel

Die Verordnung nennt einige Abklärungsmittel, welche je nach Umständen angewendet werden sollen. Dabei sind vom Kunden erhaltene Informationen grundsätzlich auf ihre Plausibilität hin zu überprüfen (Abs. 3). Informationen des Kunden (Bst. a) sind aber sowohl nützlich als auch in der Regel nötig. Den Umständen entsprechend können die auf diesem Weg erhaltenen Informationen mit Besuchen

vor Ort (Bst. b), mit der Konsultation von öffentlich zugänglichen Quellen, wie den per Internet zugänglichen Datenbanken (Bst. c), oder mit Erkundigungen bei vertrauenswürdigen Dritten (Bst. d) vervollständigt werden. Bei Letzteren kann es sich, sofern der Kunde zustimmt, auch um die ehemalige Bank des Kunden, einen anderen Kunden des Finanzintermediärs oder die auf Finanzinformationsbeschaffung spezialisierten Büros handeln. Dies bedeutet aber nicht, dass jede negative Medienmitteilung zur Folge haben soll, dass ein Kunde für einen Finanzintermediär unerwünscht ist. In Zeiten reise-rischer, teilweise unsorgfältiger und allenfalls interessengesteuerter Medienberichterstattung ist grosse Vorsicht angebracht. Der Finanzintermediär soll sich aber bei Kunden mit erhöhtem Risiko in die Lage versetzen, aufgrund einer möglichst breiten Informationsbasis eine Beurteilung vornehmen zu können (Abs. 1).

Die zusätzlichen Abklärungen müssen unter Beachtung des Persönlichkeitsschutzes des Kunden und anderer betroffener Personen erfolgen. Das bedeutet beispielsweise, dass der Finanzintermediär bei Abklärungen im Internet das Nötige vorzukehren hat, damit unbefugte Dritte ihn nicht mit dem Kunden in Verbindung bringen können (Abs. 2).

Das Resultat der zusätzlichen Abklärungen muss kritisch überprüft werden. Die vom Finanzintermediär daraus gezogenen Schlüsse müssen anschliessend dokumentiert werden (Abs. 3).

Art. 19 Delegation der zusätzlichen Abklärungen an Dritte

In aller Regel wird der Finanzintermediär die zusätzlichen Abklärungen selbst vornehmen. Es soll aber unter gewissen Voraussetzungen zulässig sein, die Abklärungen durch Dritte vornehmen zu lassen. Dies können zum Beispiel besondere Beauftragte wie Anwälte sein. Möglich ist auch, dass ein externer Vermögensverwalter die Abklärungen vornimmt. Denkbar ist auch eine Delegation innerhalb einer Finanz-

gruppe, z.B. an eine andere Gruppengesellschaft oder an den ausländischen Hauptsitz einer Zweigniederlassung in der Schweiz. Die Voraussetzungen für eine solche Delegation sind in der Verordnung geregelt. Die vorliegende Vorschrift gilt namentlich auch für Zweigniederlassungen ausländischer Banken in der Schweiz, welche die Abklärungen an den ausländischen Hauptsitz delegieren.

In der Regel finden die Bestimmungen über die Auslagerung von Geschäftsbereichen¹⁰⁷ keine Anwendung, es sei denn, ein Finanzintermediär delegiert die zusätzlichen Abklärungen dauerhaft an einen Dritten. Artikel 19 entspricht der in der VSB vorgesehenen Delegationsmöglichkeit für Kontoeröffnungen.¹⁰⁸

Die Delegation der zusätzlichen Abklärungen setzt voraus, dass der Finanzintermediär mit dem Beauftragten einen schriftlichen Vertrag abschliesst, in welchem er ihm präzise seine Aufgaben darlegt. Dies sollte unter Beachtung der drei «curae» erfolgen. Der Finanzintermediär muss sich vergewissern, dass der Beauftragte die gleiche Sorgfalt bei seiner Tätigkeit anwendet wie er (*cura in eligendo*, Bst. a). In der Schweiz sind alle dem Geldwäschereigesetz unterstellten Finanzintermediäre von Gesetzes wegen dazu verpflichtet. Der Finanzintermediär muss die notwendigen Anweisungen zur guten Ausführung der Abklärungen erteilen (*cura in instruendo*, Bst. b). Schliesslich soll er die Arbeitsqualität des Beauftragten überprüfen können (*cura in custodiendo*, Bst. c) (Absatz 1). Die Dokumentation über die Abklärungen ist dem Finanzintermediär zu übergeben. Auch in Zukunft sollen Banken und Effektenhändler die Kunden kennen, welche durch externe Vermögensverwalter und Treuhänder betreut werden (Absatz 3).

Der Finanzintermediär muss über die drei vorerwähnten *curae* hinaus noch die ihm übermittelten Informationen mit einem kritischen Auge auf ihre Plausibilität hin überprüfen, denn letztlich ist er für die gute Ausführung der Abklärungen verantwortlich (Abs. 4).

¹⁰⁷ EBK-RS 99/2.

¹⁰⁸ Abs. 19^{quater} VSB 03.

Art. 20 Zeitpunkt der zusätzlichen Abklärungen

Sind die erhöhten Risiken beim ersten Kundenkontakt ersichtlich, soll der Finanzintermediär die zusätzlichen Abklärungen sofort durchführen. In der Regel darf für die Vertragspartei vorher kein Konto operationell werden. Jedoch können die entsprechenden Abklärungen viel Zeit beanspruchen. In diesen Fällen könnte ein absolutes Verbot der Kontobenutzung während dieses Zeitraumes heikle Situationen für den Finanzintermediär hervorrufen, die nicht zwangsläufig durch die verfolgten Ziele gerechtfertigt wären, zumal doch durch die (vorläufige) Benutzung eines Kontos bis zum Vorliegen des Resultats der Abklärungen Geldwäschereiermittlungen in der Regel eher erleichtert werden, als wenn die Annahme der Vermögenswerte schlechthin verweigert würde.

Entgegen der von der VSB¹⁰⁹ gewählten Lösung wurde darauf verzichtet, einen absoluten Zeitraum zu bestimmen, innerhalb dessen das Konto nicht benutzt werden darf. Schliesslich bleibt es dem Finanzintermediär vorbehalten, die potentiellen Risiken abzuschätzen, mit denen er im entsprechenden Fall rechnen muss. Dies soll aber nicht zu endlosen Verzögerungen über Monate oder gar Jahre hinweg führen. Im mindesten sollen die Abklärungen sofort in die Wege geleitet und ohne Verzögerung ausgeführt werden, unabhängig davon, ob das Risiko am Anfang oder im Verlauf der Geschäftsbeziehung auftritt. Wenn innert vernünftiger Fristen keine aussagekräftigen Informationen beigebracht werden können, ist die Geschäftsbeziehung zu melden oder abubrechen.¹¹⁰

Art. 21 Aufnahme von Geschäftsbeziehungen mit erhöhten Risiken

Die Aufnahme einer neuen Geschäftsbeziehung mit erhöhtem Risiko verlangt die Zustimmung einer vorgesetzten Person oder Stelle. Die Aufnahme von Geschäftsbeziehungen mit PEP muss wie bis anhin auf Geschäftsleitungsebene entschieden werden.¹¹¹ Wird eine Geschäfts-

¹⁰⁹ Art. 21^{bis} VSB.

¹¹⁰ Vgl. Art. 27 f.

¹¹¹ Art. 22 Abs. 1.

beziehung erst nach einer Neubewertung als solche mit erhöhtem Risiko eingestuft, muss von der zuständigen Stelle eine Zustimmung ad-hoc eingeholt werden.

Art. 22 Verantwortung des obersten Geschäftsführungsorgans

Entscheide über Geschäftsbeziehungen mit erhöhtem Risiko sind grundsätzlich Chefsache. Nicht die unmittelbar betroffenen Kundenverantwortlichen sollen darüber entscheiden, weil es ihnen allenfalls an der notwendigen Distanz mangelt. Die oberste Geschäftsleitung darf die Verantwortung für solche zum Teil «unangenehmen» Entscheide auch nicht an untergeordnete Linienverantwortliche oder die interne Geldwäschereifachstelle abschieben können. Aufgabe der Letzteren ist es aber, die für die Geschäftsleitung notwendigen Entscheidgrundlagen zusammenzustellen.¹¹² Zu vermeiden sind umgekehrt auch Zuständigkeitsordnungen, welche die oberste Geschäftsleitung zwingen, über eine Vielzahl von Anträgen aufgrund einer Informationsfülle entscheiden zu müssen, welche sie realistisch nicht verarbeiten kann.

Im Normalfall soll deshalb, wie bereits nach den geltenden Geldwäschereirichtlinien vorgesehen, mindestens ein Mitglied der obersten Geschäftsleitung für den Entscheid darüber verantwortlich sein, ob eine Geschäftsbeziehung mit einer politisch exponierten Person aufgenommen bzw. weitergeführt werden soll. Es wird davon abgesehen, die gleiche Regelung für alle Geschäftsbeziehungen mit erhöhten Risiken vorzuschlagen, da die oberste Geschäftsleitung diese Aufgabe angesichts möglicherweise grosser Zahlen nicht in allen Fällen richtig wahrnehmen kann.¹¹³ Stattdessen soll sie aber dafür verantwortlich sein, regelmässige Kontrollen sämtlicher Geschäftsbeziehungen, die erhöhte Risiken darstellen, anzuordnen, zu überwachen und auszuwerten (Abs. 1).

Diese Zuständigkeitsordnung ist ungeeignet für grosse Banken mit

¹¹² Vgl. Art. 13 Abs. 2 Bst. g.

¹¹³ Vgl. jedoch Art. 21.

komplexen vielstufigen hierarchischen Strukturen. Hier ist im Einzelfall eine andere sachgerechte Lösung vorzusehen, welche aber dem dargestellten Grundgedanken Rechnung tragen muss (Abs. 2).

7.6 Dokumentationspflichten

Art. 23 Verfügbarkeit von Informationen

Diese Bestimmung führt Art. 7 des Geldwäschereigesetzes aus, welcher eine Pflicht zur Erstellung und zur Aufbewahrung von Dokumenten in Bezug auf Transaktionen und deren Abklärungen vorsieht. Es soll sichergestellt werden, dass sich insbesondere die Strafverfolgungsbehörden ein Bild über die Transaktionen und die entsprechenden Geschäftsbeziehungen sowie über die Einhaltung des Geldwäschereigesetzes machen können.

Buchstabe c verlangt von den Finanzintermediären auf Anfrage Informationen über Personen, die eine Vollmacht über ein Konto haben¹¹⁴, erteilen zu können. Dies bedingt in der Regel die Schaffung eines Vollmachtenregisters. Diese Forderung bezieht sich auf die Generalvollmachten mit Ausnahme der Spezialvollmachten. Überdies müssen die in einem öffentlichen Register wie dem Handelsregister publizierten Vollmachten nicht dort erscheinen. Zu dokumentieren ist auch das Resultat zusätzlicher Abklärungen bei Geschäftsbeziehungen mit erhöhten Risiken (Art. 18 Abs. 3) und Transaktionen (Art. 12 Abs. 2).

7.7 Verhalten bei Hinweisen auf Geldwäscherei oder Verbindungen mit terroristischen Organisationen

Dieser Abschnitt präzisiert und ergänzt die allgemeinen, für alle Finanzintermediäre geltenden Pflichten der Art. 9 bis 11 des Geldwäschereigesetzes. Die Regelung des Geldwäschereigesetzes, insbesondere die Bestimmungen zur Meldepflicht bei begründetem Verdacht auf Geldwäscherei, bleiben vollumfänglich anwendbar. In der Verord-

¹¹⁴ Siehe Randziffer 37 f. EBK-RS 98/1.

nung wird die Regelung im Geldwäschereigesetz aber nicht wiederholt.

Art. 24 Meldung bei Aufnahme von Geschäftsbeziehungen

Diese Bestimmung präzisiert wie die geltenden Geldwäschereirichtlinien¹¹⁵, wie sich ein Finanzintermediär bei begründetem Verdacht der Geldwäscherei oder einer Verbindung zum Terrorismus zu verhalten hat, bevor eine Geschäftsbeziehung eingegangen wird. In Anwendung von Art. 4 soll der Finanzintermediär sich weigern, ein Konto unter diesen Umständen zu eröffnen. Auch in diesem Fall muss eine Meldung im Sinne von Art. 9 des Geldwäschereigesetzes erstattet werden, sofern der Verdacht offensichtlich begründet ist.

Art. 25 Verbindungen mit einer terroristischen Organisation

Es handelt sich um eine Präzisierung der Meldepflicht im Falle eines Hinweises auf Verbindungen zu terroristischen Aktivitäten. Das Geldwäschereigesetz im Allgemeinen und Art. 9 im Speziellen sind grundsätzlich anwendbar. Entsprechend der Terrorismusfinanzierungskonvention¹¹⁶ entsteht diese Pflicht bei Vorliegen von blossen Hinweisen auf eine direkte oder indirekte Verbindung zwischen einer Transaktion oder einer Geschäftsbeziehung und einer terroristischen Organisation. Das ist insbesondere dann der Fall, wenn der Name einer der in eine Geschäftsbeziehung verwickelten Personen auf einer von den Behörden herausgegebenen Liste mutmasslicher Terroristen erscheint.

Art. 26 Verhalten bei fehlender Behördenverfügung

Dieser Artikel wiederholt und präzisiert Art. 10 Abs. 2 des Geldwäschereigesetzes im Sinne der bestehenden Regelung.¹¹⁷ Wenn die zuständigen Strafbehörden nicht innerhalb der gesetzlichen Frist eine Verfügung zustellen, soll der Finanzintermediär nach seinem Ermessen entscheiden, ob und in welchem Rahmen er die Geschäftsbezie-

¹¹⁵ Siehe Randziffer 22 EBK-RS 98/1.

¹¹⁶ Siehe Art. 18 Bst. b iii, ebenso Ziff. 4.6.

¹¹⁷ Randziffer 32 EBK-RS 98/1.

hung weiterführen will.¹¹⁸ In einem solchen Fall gelten die Bestimmungen des Zivilrechts uneingeschränkt, und der Vertragspartner ist befugt, seine Vermögenswerte zurückzuziehen oder die mit dem Finanzintermediär bestehende Vertragsbeziehung zu beenden. Um alle Zweifel auszuschliessen, wäre es wünschenswert, wenn die Strafverfolgungsbehörden die Finanzintermediäre über Gründe unterrichten würden, welche sie veranlasst haben, keine Sperre anzuordnen.

Art. 27 Zweifelhafte Geschäftsbeziehungen und Melderecht

Es kommt vor, dass Finanzintermediäre zwar keinen begründeten Verdacht haben, dass Vermögenswerte aus einem Verbrechen stammen, sie aber die Geschäftsbeziehungen aus Reputationsgründen dennoch (unter Wahrung des «paper trail» gemäss Art. 28) abbrechen möchten. Damit besteht die Gefahr, dass die Vermögenswerte auf andere schweizerische Finanzintermediäre übertragen werden, denen die Zweifel der Geschäftsbeziehung abbrechenden Finanzintermediäres jedenfalls am Anfang noch verborgen bleiben. Besonders wenn es um bedeutende Vermögenswerte geht, ist dieses unschöne Schwarzpeterspiel geeignet, dem Ansehen des Finanzplatzes ernsthaft zu schaden. In diesem Fall fordert die Verordnung die Finanzintermediäre deshalb auf, die Ausübung des Melderechts gestützt auf Art. 305^{ter} Abs. 2 StGB zu prüfen und das Resultat dieser Prüfung zu dokumentieren. Eine Meldepflicht besteht jedoch nicht.

Art. 28 Abbruch zweifelhafter Geschäftsbeziehungen

Der Finanzintermediär, der eine Geschäftsbeziehung aufgrund einfacher Zweifel abbricht und keinen Gebrauch von seinem Melderecht macht, soll die Gelder auf eine Weise transferieren, die den «paper trail» wahrt (Abs. 1), es sei denn, behördliche Blockierungsmassnahmen stünden unmittelbar bevor (Abs. 2). Dies entspricht der geltenden Regelung.¹¹⁹

¹¹⁸ Vgl. jedoch Art. 29.

¹¹⁹ Randziffer 29 EBK-RS 98/1.

Art. 29 Weiterführung zweifelhafter Geschäftsbeziehungen

Der Finanzintermediär ist natürlich berechtigt, eine zweifelhafte Geschäftsbeziehung im Sinne von Art. 27 weiterzuführen, sei es, dass er von seinem Melderecht nicht Gebrauch gemacht hat oder dass, nachdem er die Meldestelle benachrichtigt hat, ihm kein Entscheid der zuständigen Strafverfolgungsbehörden eröffnet wurde.¹²⁰ Jedoch muss aufgrund der anlässlich der Überprüfung der Melderechtsausübung gemachten Feststellungen eine schärfere Kontrolle der Geschäftsbeziehung stattfinden. Der Finanzintermediär kann ein internes Überwachungsverfahren für diese Art von Geschäftsbeziehungen vorsehen.

Art. 30 Information der Bankenkommision

Diese Bestimmung übernimmt die aktuelle Regelung.¹²¹ Nach Art. 23^{bis} Abs. 2 BankG kann die EBK von den Banken und den Revisionsstellen alle Informationen verlangen, die sie zur Erfüllung ihrer Aufgabe benötigt.

7.8 Revision

Art. 31 Prüfung durch externe Revisionsstellen

Diese Bestimmung formalisiert die Verpflichtung der externen Revisoren, im Rahmen ihrer jährlichen Revisionen die Beachtung der Verordnungsbestimmungen durch die Finanzintermediäre zu überprüfen. Die Revisionsstellen haben in ihrem ordentlichen Revisionsbericht zur Einhaltung dieser Verordnung ausdrücklich Stellung zu nehmen. Allfällige Verstösse gegen diese Verordnung (und auch gegen die VSB) sind ausdrücklich zu erwähnen. Bei Finanzgruppen ist ausdrücklich auf die nach Art. 2 der EBK-Aufsicht unterstellten Gruppengesellschaften einzugehen. Die EBK behält sich allfällige zusätzliche Schwerpunktprüfungen, ausserordentliche Revisionen oder sogar eigene Vorortkontrollen vor.

¹²⁰ Vgl. Art. 26. A fortiori, wenn die Meldestelle den Finanzintermediär informiert, dass die Meldung nicht weitergeleitet wurde.

¹²¹ Art. 34 EBK-RS 98/1.

7.9 Schlussbestimmungen

Art. 32 Übergangsbestimmungen

Die Übergangsfristen tragen der Tatsache Rechnung, dass die Verordnung im Laufe des Sommers 2002 in Vernehmlassung gegangen ist und durch die Bankenkommission in endgültiger Fassung Anfang 2003 publiziert und allen Betroffenen übermittelt wurde. Es kann jedoch nicht ausgeschlossen werden, dass sich die Anwendung der neuen Bestimmungen in einigen besonderen Fällen als schwieriger erweist als erwartet. Dies könnte insbesondere auf die Bestimmungen über zusätzliche Abklärungen bestehender Geschäftsbeziehungen zutreffen. Deshalb soll es möglich sein, ein Gesuch um Fristverlängerung an die EBK zu stellen (Absatz 1).

Die Pflicht zur Ermittlung von Geschäftsbeziehungen mit erhöhten Risiken bezieht sich auf alle Geschäftsbeziehungen und schliesst damit auch diejenigen ein, welche bei Inkrafttreten der Verordnung schon bestehen. Dafür braucht der Finanzintermediär keine rückblickende Prüfung der getätigten Transaktionen vorzunehmen (Abs. 2). Sofern zusätzliche Abklärungen noch nicht durchgeführt wurden, sind diese so rasch als möglich durchzuführen.

Die Transaktionsüberwachungssysteme müssen vom 1. Juli 2004 operativ sein und ermöglichen, entsprechend den definierten Parametern ungewöhnliche Transaktionen, die nach diesem Zeitpunkt durchgeführt werden, herauszufiltern (Abs. 3).

Um eine einfachere Bewertung der erwarteten Berichte betreffend die Umsetzung der Verordnung zu erreichen, werden die Finanzintermediäre von der EBK einen standardisierten Fragebogen erhalten, welchen sie ausfüllen und vor der Einreichung an die Bankenkommission von den externen Revisoren bestätigen lassen müssen (Abs. 4).

Es obliegt den Revisionsstellen der Finanzintermediäre, die Umset-

zung der Verordnung zu überprüfen.¹²² Die Überprüfung der Einhaltung der Verordnung ist Bestandteil der ordentlichen Prüfungstätigkeit. Die Revisionsstellen haben im Revisionsbericht zum ersten Mal für das Geschäftsjahr 2004 die Umsetzung durch die Finanzintermediäre darzustellen und im Hinblick auf die Erfüllung der Anforderungen der Verordnung zu beurteilen (Abs. 5).

Die Finanzintermediäre, die bereits der Geldwäschereiaufsicht durch die EBK im Sinne von Rz 5 der Geldwäschereirichtlinien unterstellt sind und von der Bestimmung des Art. 2 Abs. 2 profitieren möchten, haben bis Ende September 2003 bei der EBK ein entsprechendes Gesuch einzureichen. Die Gesuche müssen entsprechend den Erfordernissen von Art. 2 Abs. 2 begründet werden (Abs. 6).

¹²² Vgl. Art. 31.

Änderungen gegenüber dem Vernehmlassungsentwurf

Folgende Änderungen gegenüber dem Vernehmlassungsentwurf sind zu beachten:

- Die Verordnung verzichtet auf eine Ausweitung des Begriffs der politisch exponierten Personen (PEP) auf «ehemalige» PEP, um ehemalige PEP nicht auf Lebenszeit als Risikokunden zu kategorisieren. «Parlamentarier» wurden ebenfalls aus der Definition des PEP-Begriffs gestrichen (Art. 1 Bst. a GwV EBK).
- Die Verordnung verdeutlicht, dass es sich bei den aufgeführten Kriterien zur Erfassung von Geschäftsbeziehungen mit erhöhten Risiken nicht um eine abschliessende Aufzählung handelt, und präzisiert weiter, dass lediglich eine interne Kennzeichnung dieser Geschäftsbeziehungen verlangt wird. Als ein weiteres Kriterium wird das «Fehlen eines persönlichen Kontakts zur Vertragspartei und zum wirtschaftlich Berechtigten» aufgeführt (Art. 7 GwV EBK).
- Als ein weiteres Kriterium für Transaktionen mit erhöhten Risiken werden «erhebliche Abweichungen gegenüber den in vergleichbaren Geschäftsbeziehungen üblichen Transaktionsarten, -volumina und -frequenzen» aufgeführt (Art. 8 GwV EBK).
- Bei der Delegation von zusätzlichen Abklärungen an Dritte hat der Finanzintermediär sich zu vergewissern, dass die beauftragten Personen und Unternehmen dieselbe Sorgfalt anwenden wie er selbst. Er hat sie über ihre Aufgaben zu instruieren und muss die sorgfältige Durchführung der Abklärungen kontrollieren können. Eine Weiterdelegation durch den Beauftragten ist verboten. Der Finanzintermediär hat die Ergebnisse der Abklärungen selber auf ihre Plausibilität hin zu überprüfen (Art. 19 GwV EBK).
- Die Verordnung verlangt, dass der Finanzintermediär bei zweifelhaften Geschäftsbeziehungen, insbesondere wenn sie bedeutende Ver-

mögenswerte betreffen, die Ausübung des strafrechtlichen Melde-
rechts prüft und das Resultat der Prüfung dokumentiert (Art. 27
GwV EBK).

- Die bereits im Rundschreiben 98/1 enthaltene Bestimmung zur Weiterführung der Geschäftsbeziehung unter besonderer Kontrolle wird in der Verordnung wieder aufgenommen (Art. 29 GwV EBK).
- Der Finanzintermediär hat die EBK über Meldungen an die Meldestelle zu informieren, die Geschäftsbeziehungen mit bedeutenden Vermögenswerten betreffen oder wenn aufgrund der Umstände anzunehmen ist, dass der Fall Auswirkungen auf den Ruf des Finanzintermediärs oder des Finanzplatzes haben könnte (Art. 30 GwV EBK).
- Die Verordnung statuiert ausdrücklich, dass die Einhaltung der Verordnung der Prüfung durch die externen Revisionsstellen unterliegt und eine entsprechende Stellungnahme im Revisionsbericht enthalten sein muss (Art. 31 GwV EBK).

Rapport CFB sur le blanchiment

Rapport de la Commission fédérale des banques relatif à son ordonnance sur le blanchiment d'argent du 18 décembre 2002

Mars 2003

Avant-propos

Ce rapport se fonde principalement sur celui du «Groupe de travail KYC» publié en juillet 2002 simultanément à l'ouverture de la consultation sur le projet d'ordonnance de la CFB sur le blanchiment¹. Il a toutefois été actualisé et adapté aux développements intervenus depuis lors ainsi qu'aux modifications² apportées par la CFB suite à la consultation.

Les notes explicatives contenues dans le présent rapport n'ont pas la prétention de répondre à toutes les questions de détails qui se poseront pour les banques dans le cadre de la (difficile) mise en œuvre de la nouvelle réglementation. Elles ont uniquement pour but de mettre quelque peu en lumière le contexte et d'expliquer sur certains points d'importance quel but une disposition poursuit ou (ce qui peut parfois être tout aussi important) ne poursuit justement pas. Les incertitudes subsistantes seront à régler dans le cadre d'un dialogue entre la CFB, les banques et les réviseurs. Dans la mesure du possible, la CFB souhaite éviter la mise en place de réglementations additionnelles sur des détails mineurs et faire usage de son pouvoir régulateur uniquement dans la mesure où cela s'impose afin de garantir un minimum d'uni-

¹ «Devoirs de diligence des banques et des négociants en matière de blanchiment d'argent, de financement du terrorisme et de relations d'affaires avec des personnes politiquement exposées», Rapport d'un Groupe de travail institué par la Commission fédérale des banques relatif au projet d'une ordonnance de la Commission fédérale des banques, juin 2002, disponible sur le site internet de la CFB:

<http://www.ebk.admin.ch/f/archiv/2002/neu090702-02f.pdf>.

² Cf. annexe I.

formité dans l'application de la loi. L'Ordonnance applique une approche différenciée en fonction du risque. Dès lors que les risques sont différents pour chaque intermédiaire financier, les solutions dans la mise en œuvre de l'Ordonnance le seront nécessairement aussi. La CFB ne souhaite pas se départir de cette approche différenciée dans le cadre de l'application de cette réglementation.

Table des matières

1	Survol	168
2	Révision de la réglementation actuelle	172
2.1	Situation initiale	172
2.2	Groupe de travail KYC	173
2.3	Consultation	174
3	Cadre national	177
3.1	Développements de la législation	178
3.2	Cadre institutionnel	180
3.3	Surveillance et rôle de la CFB	181
3.4	Autorégulation des banques	183
4	Développements internationaux	184
4.1	Les 40 Recommandations du GAFI (juin 1996)	184
4.2	Recommandations du GAFI sur le financement du terrorisme (octobre 2001)	185
4.3	Convention pour la répression du financement du terrorisme (décembre 1999)	186
4.4	Principes de Wolfsberg (2000 / 2002)	186
4.5	«Customer Due Diligence paper» du Comité de Bâle (octobre 2001)	187
4.6	«Supervisors' PEP working paper 2001» (novembre 2001)	188
4.7	Autres instruments internationaux d'importance	188
4.8	FMI – Financial Sector Assessment Switzerland (juin 2002)	189
5	Grandes lignes de l'Ordonnance	190
5.1	Ordonnance en remplacement des Directives de la CFB sur le blanchiment de capitaux	190
5.2	Délimitation matérielle par rapport à l'autorégulation	191
5.3	Développement des règles sur les personnes politiquement exposées	192
5.4	Devoir de diligence différencié en fonction des risques	193
5.5	Surveillance systématisée des transactions	194
5.6	E-Banking	195
5.7	Gestion globale des risques de réputation	196
5.8	Lutte contre le financement du terrorisme	197

6	Convention de diligence	198
7	Commentaire de l'Ordonnance	200
7.1	Dispositions générales	200
7.2	Principes	204
7.3	Mesures organisationnelles	206
7.4	Obligations de diligence générales	214
7.5	Obligations de diligence accrues	216
7.6	Devoirs de documentation	222
7.7	Comportement en présence d'indices de blanchiment ou de liens avec des organisations terroristes	223
7.8	Révision	225
7.9	Dispositions finales	226
	Annexe I: Principales modifications par rapport au projet soumis en consultation	228

Liste des abréviations

ASB	Association suisse des banquiers
Autorité de contrôle	Autorité de contrôle en matière de lutte contre le blanchiment d'argent
Bureau de communication	Bureau de communication en matière de blanchiment
CDB, Convention de diligence	Convention relative à l'obligation de diligence des banques du 28 janvier 1998
CFB, Commission des banques	Commission fédérale des banques
CDD	«Customer Due Diligence for Banks» émis en octobre 2001 par le Comité de Bâle
Comité de Bâle	Comité de Bâle sur le contrôle bancaire
Convention sur le financement du terrorisme	Convention internationale pour la répression du financement du terrorisme du 9 décembre 1999
CP	Code pénal suisse du 21 décembre 1937 (RS 311.0)
Directives sur le blanchiment de capitaux	Directives relatives à la prévention et à la lutte contre le blanchiment de capitaux (Circ.-CFB 98/1)
FMI	Fonds Monétaire International
GAFI	Groupe d'Action Financière sur le blanchiment de capitaux
LB, Loi sur les banques	Loi fédérale sur les banques et les caisses d'épargne du 8 novembre 1934 (RS 952.0)
LBA, Loi sur le blanchiment	Loi fédérale concernant la lutte contre le blanchiment d'argent dans le secteur financier du 10 octobre 1997 (RS 955.0)
LBVM, Loi sur les bourses	Loi fédérale sur les bourses et le commerce des valeurs mobilières du 24 mars 1995 (RS 954.1)
LFP, Loi sur les fonds de placement	Loi fédérale sur les fonds de placement du 18 mars 1994 (RS 951.31)
Message	Message du Conseil fédéral

OBA-CFB, Ordonnance	Ordonnance de la Commission fédérale des banques en matière de lutte contre le blanchiment d'argent du 18 décembre 2002
Ordonnance de l'Autorité de contrôle	Ordonnance de l'Autorité de contrôle concernant les obligations de diligence des intermédiaires financiers qui lui sont directement soumis (RS 955.033.2)
P-CP	Modification du code pénal suisse et du code pénal militaire du 14 décembre 2002 (Feuille Fédérale 1999 1787; RS 311.0)
PEP	Politically Exposed Persons: personnes politiquement exposées

1 Survol

En tant qu'autorité de surveillance instituée par une loi spéciale au sens de la loi sur le blanchiment, la CFB surveille le respect des devoirs résultant de la loi sur le blanchiment par les établissements qui lui sont assujettis. L'art. 41 de la loi sur le blanchiment octroie à la CFB la compétence d'édicter des dispositions d'exécution.

En avril 2001, la CFB avait chargé un groupe de travail d'engager une révision de la réglementation alors en vigueur. Celui-ci a déposé un projet d'ordonnance d'exécution de la loi sur le blanchiment en juin 2002 qui devait remplacer les Directives sur le blanchiment de capitaux de la CFB³. Après une procédure de consultation publique, l'Ordonnance a été adoptée par la CFB le 18 décembre 2002 et entrera en vigueur le 1^{er} juillet 2003.

Alors que l'Ordonnance détermine les devoirs de diligence applicables aux relations d'affaires comportant des risques accrus (art. 6 LBA), la Convention de diligence de l'ASB qui a également fait l'objet d'une révision⁴ règle comme cela était le cas jusqu'à présent les principes applicables à l'identification pour toutes les relations. En comparaison avec la réglementation actuelle, l'Ordonnance contient les nouveautés principales suivantes:

- En matière de prévention du blanchiment, les intermédiaires financiers utilisent une approche différenciée en fonction du risque. Des clarifications complémentaires sont exigées concernant les relations d'affaires comportant des risques accrus, par exemple sur la provenance des valeurs patrimoniales. Cela implique que les intermédiaires financiers aient établi auparavant, conformément à leurs domaines d'activités, une liste de critères de risques et que, sur cette base, ils aient identifié toutes les relations d'affaires (préexistantes

³ Cf. note 1 supra.

⁴ Convention de diligence des banques 2003, disponible sur l'internet: <http://www.swissbanking.org/fr/cdb-03-140103-mit-formularen.pdf>.

ou nouvelles) comportant des risques accrus. Les relations ainsi déterminées doivent être désignées comme telles pour l'usage interne. En dehors de la procédure ordinaire d'identification au sens de la Convention de diligence CDB, aucune clarification complémentaire n'est en revanche exigée pour les relations d'affaires restantes.

- L'Ordonnance reprend la réglementation actuelle en matière de relations avec des personnes politiquement exposées. La décision d'admettre, de poursuivre ou de rompre de telles relations d'affaires doit être prise par la direction à son plus haut niveau. Il est interdit d'accepter des valeurs patrimoniales dont l'intermédiaire financier sait ou doit présumer qu'elles proviennent d'un crime, que celui-ci ait été commis en Suisse ou à l'étranger. Cet interdit s'applique en particulier également aux valeurs patrimoniales qui proviennent de la corruption ou du détournement de fonds publics.
- Les instruments qui étaient jusqu'à présent utilisés uniquement dans le cadre de la lutte contre le blanchiment le seront maintenant aussi dans la lutte contre le financement du terrorisme⁵. Lorsque les clarifications de l'arrière-plan économique de transactions inhabituelles ou suspectes révèlent un lien avec une organisation terroriste, l'intermédiaire financier doit immédiatement effectuer une communication au Bureau de communication.
- En cas de doutes au sujet de la qualité d'une relation d'affaires, les intermédiaires financiers doivent examiner s'ils veulent faire usage de leur droit de communiquer et transmettre leurs indices au Bureau de communication. Ce principe est en particulier valable dans le cas de relations d'affaires comportant d'importantes valeurs patrimoniales.
- A l'exception d'établissements de petite taille, les banques et les négociants sont tous tenus de mettre en place un système informatisé de surveillance des transactions devant servir à la détection de transactions inhabituelles. Ces dernières doivent ensuite être examinées dans un délai raisonnable. Cas échéant, des clarifications complémentaires relatives à la relation d'affaires doivent être entreprises.

⁵ Cf. ch. 5.8 infra.

- En application des standards développés par le Groupe d'Action Financière sur le blanchiment (GAFI) en matière de lutte contre le financement du terrorisme, tous les virements à destination de l'étranger doivent contenir des informations sur le cocontractant donneur d'ordre.
- L'Ordonnance formalise le régime des Directives sur le blanchiment de capitaux et englobe expressément, en sus des banques et des négociants, également les sociétés qui appartiennent à une banque ou à un négociant sans disposer elles-mêmes d'un statut de banque ou de négociant. Ces sociétés peuvent, sur la base d'une demande formelle, requérir leur assujettissement à la surveillance de la CFB pour ce qui est du respect des devoirs de diligence statué dans l'Ordonnance. Les requêtes pour des sociétés de groupe qui, au moment de l'entrée en vigueur de l'Ordonnance, exercent une activité au sens de l'art. 2 al. 3 de la loi sur le blanchiment et qui souhaitent être assujetties à la surveillance de la CFB en matière de blanchiment, doivent être déposées auprès de la CFB jusqu'à fin septembre 2003. Les requêtes concernant plusieurs sociétés d'un même groupe financier peuvent être regroupées et déposées de manière centrale par le groupe.
- L'Ordonnance explicite la règle de la circulaire actuelle selon laquelle il est interdit aux intermédiaires financiers suisses d'utiliser leurs entités étrangères afin de contourner la réglementation suisse. L'Ordonnance exige des intermédiaires financiers qu'ils veillent à ce que leurs entités étrangères se conforment aux principes fondamentaux de l'Ordonnance. Dans l'hypothèse où les normes suisses ne correspondent pas au droit du pays d'accueil ou à la pratique de celui-ci, les groupes bancaires suisses peuvent en subir un désavantage concurrentiel. Dans de tels cas, la CFB devra trouver des solutions individuelles en accord avec les autorités de surveillance compétentes et les établissements concernés.
- Les intermédiaires financiers qui possèdent des succursales ou des sociétés à l'étranger doivent déterminer, limiter et contrôler de ma-

nière globale leurs risques juridiques et leurs risques de réputation. Ils doivent s'assurer que les succursales et sociétés du groupe à l'étranger transmettent aux organes compétents du groupe les informations essentielles à cet effet. Les organes de contrôle internes et les réviseurs externes du groupe doivent pouvoir disposer, en cas de besoin, d'un accès aux informations relatives à des relations d'affaires individuelles de chaque succursale et société du groupe.

- Les dispositions de l'Ordonnance sont applicables aux relations de correspondance bancaire également. Aucun compte ne peut être tenu pour des banques sans présence physique au lieu de leur incorporation («shell banks»), à moins qu'il ne s'agisse de filiales de groupes financiers faisant l'objet d'une surveillance consolidée adéquate.
- L'Ordonnance intègre les dispositions actuellement contenues dans la circulaire du 6 avril 1990 sur la réglementation du commerce professionnel de billets de banque dans les banques⁶.

A l'entrée en vigueur de l'Ordonnance au 1^{er} juillet 2003, sont abrogés:

- Les directives de la CFB du 6 avril 1990 sur la réglementation du commerce professionnel de billets de banque dans les banques;
- Les standards minimaux de la CFB applicables aux banques et négociants actifs exclusivement sur l'internet du 29 mars 2001. Les banques et négociants concernés devront toutefois appliquer ces standards minimaux jusqu'à ce que les prescriptions correspondantes de l'Ordonnance et de la Convention de diligence 2003 soient applicables.

La circulaire 98/1 de la CFB du 26 mars 1998 (Directives relatives à la prévention et à la lutte contre le blanchiment de capitaux) est abrogée au 30 juin 2004. Jusqu'à cette date, les prescriptions de l'Ordonnance pour lesquelles il n'existe pas de délai transitoire prévalent.

⁶ Bulletin CFB 20, 1990, p. 101.

L'Ordonnance prévoit un délai transitoire d'un an, soit jusqu'à fin 2004, pour la mise en œuvre de certaines dispositions. Jusqu'à cette date, les intermédiaires financiers doivent entre autres déterminer toutes les relations d'affaires existantes qui comportent des risques accrus et les désigner comme telles pour l'usage interne. Tous les devoirs résultant de l'Ordonnance pour lesquels aucun délai transitoire n'est spécifié acquièrent force obligatoire au 1^{er} juillet 2003.

L'Ordonnance exige des intermédiaires financiers qu'ils fassent rapport à la CFB sur l'avancement de la mise en œuvre à fin septembre 2003. Devront être soumis un concept de mise en œuvre ainsi qu'un calendrier y relatif, accompagnés d'une confirmation par les réviseurs externes. Au printemps 2003, la CFB fera parvenir à tous les intermédiaires financiers concernés un questionnaire à utiliser à cette fin. Elle n'a pas l'intention d'évaluer individuellement les concepts et les systèmes de surveillance des transactions. Elle tient simplement à s'assurer que la mise en œuvre de l'Ordonnance est en bonne voie et n'interviendra qu'en cas de problèmes de nature fondamentale.

2 Révision de la réglementation actuelle

2.1 Situation initiale

La CFB a édicté en 1991 ses premières Directives sur le blanchiment de capitaux⁷, suite à l'entrée en vigueur des dispositions du Code pénal sur le blanchiment d'argent⁸ et le défaut de vigilance en matière d'opérations financières⁹. Ces directives ont fait l'objet d'une révision totale en 1998¹⁰, en particulier afin de prendre en compte les développements des standards internationaux dans le domaine de la lutte contre le blanchiment¹¹.

⁷ Circ.-CFB 91/3.

⁸ Art. 305^{bis} CP.

⁹ Art. 305^{ter} CP.

¹⁰ Circ.-CFB 98/1.

¹¹ Voir énumération sous ch. 2 Circ.-CFB 98/1.

Dans les années 2000 et 2001, les affaires Abacha et Montesinos¹², dans lesquelles furent également impliquées certaines banques suisses, suscitèrent une publicité aussi bien au niveau national qu'international. A cette occasion, se posa la question de la nécessité d'un renforcement de la réglementation en vigueur. La CFB considéra que celle-ci était fondamentalement adéquate, une adaptation étant toutefois nécessaire sur certains points. Elle décida en conséquence d'entreprendre une révision des Directives sur le blanchiment de capitaux. L'entrée en vigueur en mai 2000 d'une nouvelle disposition pénale réprimant la corruption de fonctionnaires étrangers livra un motif supplémentaire à cette révision¹³. Enfin, les développements récents des standards internationaux en matière de lutte contre le blanchiment devaient également être pris en compte dans le cadre de cette révision.

2.2 Groupe de travail KYC

En avril 2001, la CFB chargea un groupe de travail («Groupe de travail KYC») de la révision des Directives sur le blanchiment de capitaux. Ce groupe de travail comprenait des représentants de l'Association suisse des banquiers, de l'Association suisse des négociants indépendants, de la Commission de surveillance CDB, de la Chambre fiduciaire suisse, de la Swiss Association of Compliance Officers, des autorités cantonales de poursuite pénale, de l'Autorité de contrôle et du Bureau de communication. Il était présidé par M. Urs Zulauf, sous-directeur du Secrétariat de la CFB.

Selon décision de la CFB, ce groupe de travail devait en particulier vérifier dans quelle mesure les Directives sur le blanchiment de capitaux qui reposent essentiellement sur le principe «one size fits all», devaient être remplacées par une réglementation différenciée et si des devoirs de diligence plus sévères et des obligations de contrôle spé-

¹² Voir l'information à l'intention des médias par la CFB dans les affaires Abacha et Montesinos sous <http://www.ebk.admin.ch/f/archiv/2000/archiv2000.htm>; <http://www.ebk.admin.ch/f/archiv/2001/archiv2001.htm>.

¹³ Art. 322^{septies} CP, en vigueur depuis le 1^{er} mai 2000.

ciales devaient valoir dans le domaine du Private Banking. Le mandat du groupe de travail portait également sur les questions de savoir s'il y avait lieu de poser des exigences particulières dans le cas de relations entre absents ou dans le domaine e-banking. Par ailleurs, il s'agissait de déterminer les conditions auxquelles une délégation des clarifications devait être admise. En juin 2002, le groupe de travail remit à la CFB un projet d'ordonnance reposant sur la loi sur le blanchiment d'argent, accompagné d'un rapport explicatif¹⁴.

2.3 Consultation

En juillet 2002, la CFB publia le projet du groupe de travail KYC aux fins de consultation et invita tous les cercles intéressés à lui faire parvenir leur prise de position. Le projet fut généralement accueilli de manière positive. Les participants à la consultation saluèrent en particulier l'approche différenciée en fonction des risques en matière de prévention du blanchiment, désormais inscrite dans l'Ordonnance. Certaines propositions du groupe de travail furent toutefois l'objet de critiques:

- Certains participants à la consultation critiquèrent l'application extraterritoriale de l'Ordonnance aux succursales et sociétés de groupes à l'étranger. Malgré ces réserves, la CFB s'est décidée à garder la disposition selon laquelle les intermédiaires financiers doivent veiller à ce que leurs succursales et sociétés de groupe à l'étranger se conforment aux principes fondamentaux de l'Ordonnance. Cette disposition tend à préciser l'interdiction de contourner la réglementation contenue dans l'actuelle circulaire. Elle repose sur le principe selon lequel la lutte contre le blanchiment n'est effective que dans la mesure où un dispositif défensif satisfaisant aux exigences suisses est mis en place dans les succursales et les sociétés de groupe à l'étranger. Par cette réglementation, la CFB souhaite éviter la survenance de conflits de compétence en matière de surveillance.

¹⁴ Cf. note 1 supra.

- L'obligation de mettre en place une gestion globale des risques juridiques et des risques de réputation à l'intérieur d'un groupe financier fut également critiquée. Celle-ci nécessitait en effet un échange d'informations au sein du groupe, soit au-delà des frontières nationales, ce que la situation juridique dans de nombreux pays ne permettrait pas ou limiterait fortement. La CFB a décidé de conserver cette disposition également. Dès lors que les risques de réputation ne connaissent pas de frontières, les organes responsables du groupe doivent connaître les relations d'affaires importantes comportant des risques accrus. A cette fin, un transfert des informations essentielles pertinentes doit être possible dans les deux sens et cela aussi bien depuis la société de groupe étrangère vers la société-mère suisse qu'inversément. La CFB est tout à fait consciente de l'existence de certains obstacles aux flux d'informations transfrontières, raison pour laquelle un devoir d'information correspondant a été prévu pour les cas dans lesquels les informations nécessaires ne seraient pas accessibles à l'étranger. Pour les succursales suisses de banques étrangères et les sociétés suisses de groupes étrangers, cette disposition s'appuie sur l'art. 4^{quinquies} de la loi sur les banques selon lequel toutes les informations nécessaires à la surveillance consolidée peuvent être transmises à la société-mère étrangère.
- L'élargissement – prévu dans le projet – de la notion de PEP aux anciens PEP ne trouva pas de soutien suffisant auprès des participants à la consultation. Afin d'éviter de cataloguer à vie comme PEP les personnes occupant des fonctions publiques importantes, l'Ordonnance renonce à cet élargissement. Par ailleurs, pour éviter d'étendre de manière excessive le champ de la définition des PEP, ce qui aurait également été contraire à l'approche différenciée en fonction du risque, l'Ordonnance renonce de même à soumettre les PEP nationaux à cette réglementation, contrairement au souhait de certains participants à la consultation. Les personnes occupant des fonctions publiques importantes au niveau régional ainsi que les parlementaires ne sont pas non plus compris dans la définition. En revanche,

les principes généraux de la prévention du blanchiment ancrés dans l'Ordonnance, soit l'interdiction générale d'accepter des valeurs patrimoniales provenant de la corruption ou d'un autre crime, sont applicables. L'Ordonnance exige de tous les intermédiaires financiers qu'ils développent des critères pertinents pour la détection des relations d'affaires comportant des risques juridiques accrus ou des risques de réputation accrus, et propose à cet effet une liste non exhaustive de critères possibles. En application de ces critères, certaines relations d'affaires nouées avec des PEP nationaux peuvent aussi être qualifiées comme comportant des risques accrus. Contrairement à ce qui prévaut en matière de relations avec des PEP étrangers, cette classification n'est toutefois pas contraignante. Il est loisible à un intermédiaire financier de répertorier tous les PEP nationaux ou certains d'entre eux dans la catégorie des risques accrus et de leur appliquer des devoirs de diligence additionnels. Par ailleurs, lorsqu'un PEP national fait exécuter une transaction qui est identifiée comme inhabituelle, une diligence additionnelle est requise de même que lors de toute autre transaction inhabituelle.

- De nombreux participants à la consultation exprimèrent des réserves à l'égard du devoir de faire figurer le nom et le numéro de compte des donneurs d'ordre de paiement. Les représentants des banques jugent que d'importants risques existent du point de vue de la sécurité si le nom et le numéro de compte du donneur d'ordre apparaissent sur les documents de transaction. Selon leur opinion, un risque d'abus de ces informations (Identity fraud) existerait en particulier lors d'un transfert au travers de plusieurs banques correspondantes, en raison du fait que le numéro de compte et le nom du titulaire de celui-ci serait ensuite connu d'un nombre élevé de personnes, soit toutes celles qui participent à l'exécution de l'opération. L'Ordonnance tient compte de ces réserves émises pour des raisons de sécurité dans la mesure où elle autorise le remplacement du numéro de compte par un numéro d'identification.
- Certains participants à la consultation se sont prononcés contre la

proposition de la CFB de prévoir une obligation de rencontrer le client. Ce contact n'est en effet pas toujours possible, en particulier dans certains domaines d'activité (p.ex. e-banking) ou avec certains clients étrangers. En lieu et place d'un devoir général de rencontrer le client, l'Ordonnance prévoit maintenant l'absence de contact personnel avec le client au nombre des critères signalant la présence de risques accrus pour les relations d'affaires et entraînant des clarifications complémentaires.

- La question des délais transitoires se révéla un des points principaux sur lesquels la critique se focalisa. De nombreux participants à la consultation se prononcèrent contre la volonté exprimée par la CFB de raccourcir le délai transitoire d'un an. Ils demandèrent au contraire une prolongation de celui-ci, en particulier pour mener à bien la classification des relations d'affaires existantes dans les catégories de risques que pour l'introduction de systèmes de surveillance des transactions. La CFB a renoncé à raccourcir le délai transitoire. De même, elle a décidé de ne pas prolonger celui-ci, se réservant la possibilité d'octroyer une prolongation aux intermédiaires financiers, au cas par cas et sur requête motivée.

La majorité des observations et propositions de détail faites dans le cadre de la consultation ont été prises en compte lors de l'élaboration de la présente version de l'Ordonnance qui a été adoptée le 18 décembre 2002 par la CFB. Les modifications de l'Ordonnance par rapport au projet soumis en consultation n'affectent toutefois en rien les nouveautés centrales de l'Ordonnance par rapport à la réglementation actuelle¹⁵.

3 Cadre national

L'Ordonnance de la CFB ne constitue qu'un des piliers du système suisse de défense en matière de lutte contre le blanchiment d'argent et

¹⁵ Pour une énumération des principales modifications par rapport au projet soumis en consultation, voir Annexe I.

contre le financement du terrorisme, lequel se compose d'un élément préventif et d'un élément répressif respectivement matérialisés dans le droit administratif et le droit pénal. Le développement de la réglementation de la CFB est par conséquent en relation étroite avec les modifications législatives et institutionnelles qui se sont produites en Suisse ces dernières années dans le domaine de la lutte contre le blanchiment d'argent et qui sont décrites ci-après.

3.1 Développements de la législation

Depuis le début des années '80, une série de dispositions d'ordre pénal, prudentiel et conventionnel ont été introduites sur un plan national pour renforcer le système de lutte contre le blanchiment d'argent. Dans le domaine du droit pénal, les dispositions du Code pénal¹⁶ relatives au blanchiment d'argent et au défaut de vigilance en matière d'opérations financières sont entrées en vigueur le 1^{er} août 1990. Tombent sous le coup du blanchiment d'argent, tous les actes propres à entraver l'identification de l'origine, la découverte ou la confiscation de valeurs patrimoniales provenant d'un crime¹⁷. Le défaut de vigilance en matière d'opérations financières se rapporte en particulier à l'omission de l'identification de l'ayant droit économique¹⁸. Le droit de communication introduit en août 1994 autorise les intermédiaires financiers à communiquer aux autorités des informations ou constatations qui permettent de conclure que les valeurs patrimoniales concernées proviennent d'un crime¹⁹.

En dehors de ces dispositions, d'autres normes pénales sont pertinentes du point de vue du blanchiment en tant que conditions d'application de la Loi sur le blanchiment. A cet égard, il faut mentionner les dispositions relatives à la lutte contre la criminalité organisée²⁰ en-

¹⁶ Code pénal suisse du 21 décembre 1937 (RS 311.0), disponible sur l'internet sous http://www.bk.admin.ch/ch/fr/rs/c311_0.html.

¹⁷ Art. 305^{bis} CP.

¹⁸ Art. 305^{ter} CP.

¹⁹ Art. 305^{ter} al. 2 CP.

²⁰ Art. 260^{ter} ch. 1 CP.

trées en vigueur le 1^{er} août 1994 ainsi que le droit pénal de la corruption²¹. En application de la Convention de l'OCDE sur la lutte contre la corruption d'agents publics étrangers dans les transactions commerciales internationales²², est maintenant aussi punissable la corruption d'agents publics étrangers²³. L'introduction d'une responsabilité pénale pour les personnes morales prévue dans le cadre de la prochaine modification du Code pénal est également d'importance en matière de répression du blanchiment²⁴. Cette norme prévoit une responsabilité de l'entreprise en raison de manquements dans l'organisation de celle-ci dans deux cas. En premier lieu et de manière pour ainsi dire subsidiaire, pour des crimes ou délits de droit commun, lorsque l'acte incriminé ne peut être imputé à aucune personne physique au sein de l'entreprise du fait d'une organisation défectueuse de celle-ci. En second lieu et de manière primaire, lorsque, dans le cas de certaines infractions spécifiques, l'entreprise n'a pas pris toutes les mesures nécessaires qui pouvaient raisonnablement être attendues d'elle pour empêcher la survenance de ces infractions. Une norme pénale spéciale devrait être créée dans le cadre de la mise en œuvre de la Convention pour la suppression du terrorisme²⁵.

La Loi sur le blanchiment²⁶ entrée en vigueur le 1^{er} avril 1998 complète les dispositions précitées du Code pénal. Elle s'applique à l'ensemble du secteur financier. Est déterminante à cet égard la notion d'intermédiaire financier qui comprend, outre les intermédiaires financiers soumis avant l'entrée en vigueur de ladite loi à une surveillance en vertu de lois spéciales, tels les banques, les assurances, les négociants

²¹ Cf. art. 322^{quater} (corruption active) et art. 322^{ter} (corruption passive) CP.

²² Cf. note 62 *infra*.

²³ Art. 322^{septies} CP.

²⁴ Cf. art. 102 et 102a P-CP. Modification du 13 décembre 2002 disponible sur l'internet: <http://www.ofj.admin.ch/f/index.html> (sous législation, partie générale du CP). Voir aussi Message concernant la modification du code pénal suisse (dispositions générales, entrée en vigueur et application du code pénal) et du code pénal militaire ainsi qu'une loi fédérale régissant la condition pénale des mineurs du 21 septembre 1998 (FF 1999 1787), disponible sur l'internet: <http://www.ofj.admin.ch/f/index.html>.

²⁵ Cf. ch. 4.2 et 5.8 *infra*.

²⁶ Disponible sur l'internet: http://www.bk.admin.ch/ch/f/rs/c955_0.html.

en valeurs mobilières et les directions de fonds, également les avocats, notaires, la poste, les négociants de métaux précieux et les bureaux de change notamment. La loi impose aux intermédiaires financiers des obligations de nature organisationnelle concernant la formation du personnel et les contrôles internes par exemple, de même que des obligations au niveau de leur fonctionnement, telles la vérification de l'identité du cocontractant, l'identification de l'ayant droit économique, la clarification de l'arrière-plan économique d'une transaction en présence d'indices de blanchiment et l'obligation de conserver la documentation. Du point de vue des banques, cette nouvelle législation n'a toutefois pas apporté de changements en raison du fait que ces devoirs découlaient déjà, pour le secteur bancaire, en partie de la Convention de diligence²⁷ et en partie des Directives sur le blanchiment de capitaux²⁸.

3.2 Cadre institutionnel

La Loi sur le blanchiment a créé deux nouvelles autorités fédérales qui s'ajoutent aux autorités de surveillance déjà en place en vertu des lois spéciales: l'Autorité de contrôle²⁹ et le Bureau de communication³⁰. Ces nouvelles autorités ont notamment pour tâche de veiller à l'exécution des mécanismes de contrôle. Par ailleurs, la loi confère certaines compétences étatiques en matière de contrôle à des organismes d'autorégulation³¹.

Du point de vue administratif, l'Autorité de contrôle est rattachée au Département fédéral des finances. Sont soumis à son autorité tous les intermédiaires financiers, à l'exception de ceux qui font l'objet d'une

²⁷ Cf. Note 38 infra.

²⁸ Circ.-CFB 91/3, Directives sur le blanchiment de capitaux du 18 décembre 1991; cf. également Rapport de gestion CFB 1991, p. 219 ss. Cette circulaire a été remplacée par la Circ.-CFB 98/1 du 26 mars 1998 qui est en vigueur depuis le 1^{er} juillet 1998.

²⁹ Art. 17–22 LBA; cf. également le site internet de l'Autorité de contrôle sous <http://www.gwg.admin.ch/>.

³⁰ Art. 23 LBA; cf. également le site internet du Bureau de communication sous http://internet.bap.admin.ch/d/themen/geld/i_index.htm.

³¹ Art. 24–28 LBA.

surveillance par la CFB ou l'Office fédéral des assurances privées en vertu d'une loi spéciale. Les intermédiaires financiers doivent s'affilier à un organisme d'autorégulation ou requérir leur assujettissement directement de l'Autorité de contrôle. Dans le premier de ces cas de figure, celle-ci exerce une surveillance indirecte par le biais de son contrôle sur les organismes d'autorégulation. En cas de violation des devoirs imposés par la Loi sur le blanchiment, les organismes d'autorégulation peuvent prononcer des sanctions à l'encontre de leurs membres, lesquelles peuvent revêtir la forme de peines conventionnelles. L'Autorité de contrôle peut ordonner des mesures à l'encontre des organismes d'autorégulation aussi bien que des intermédiaires financiers qui lui sont directement assujettis. Dans des cas graves, elle peut retirer la reconnaissance à un organisme d'autorégulation ou l'autorisation à un intermédiaire financier et liquider ce dernier.

Au-delà des devoirs de diligence à proprement parler, la Loi sur le blanchiment prévoit l'obligation de communiquer les cas de soupçons fondés de blanchiment au Bureau de communication ainsi que de bloquer les valeurs patrimoniales concernées. Le Bureau de communication est rattaché à l'Office fédéral de la police. Sa tâche consiste à recueillir et évaluer les informations transmises par les intermédiaires financiers en application de la Loi sur le blanchiment. Les cas de soupçons fondés de blanchiment sont immédiatement dénoncés aux autorités chargées de la poursuite pénale. La compétence d'investigation dans le domaine du blanchiment ainsi que dans ceux du crime organisé, de la corruption et de la criminalité économique majeure a été conférée à la Confédération dans le cadre du Projet d'efficacité³².

3.3 Surveillance et rôle de la CFB

Il incombe à la CFB de contrôler l'observation des obligations découlant de la Loi sur le blanchiment par les établissements soumis à sa

³² Nouvelles compétences de procédure en faveur de la Confédération dans les domaines du crime organisé et de la criminalité économique. Modification du 22 décembre 1999, disponible sur l'internet sous <http://www.admin.ch/ch/f/as/2001/3071.pdf>. La réglementation est en vigueur depuis le 1^{er} janvier 2002.

surveillance. Pour certaines de ces obligations, par exemple la clarification de l'arrière-plan économique de transactions complexes importantes et inhabituelles³³, la Commission des banques avait déjà développé une pratique depuis la fin des années '70 sur la base de l'exigence de la garantie d'une activité irréprochable statuée dans la Loi sur les banques³⁴. En relation avec l'affaire Marcos, la Commission des banques précisait sa pratique selon laquelle la décision de l'acceptation ou de la poursuite d'une relation d'affaires avec des PEPs relevait de la direction de la banque, à l'exclusion d'instances subalternes. Cette pratique a fait l'objet d'une première publication dans le Rapport de gestion 1987³⁵ et a été précisée suite aux affaires Mobutu et Benazir Bhutto au cours de l'année 1997³⁶. Ces règles ont été formalisées dans le cadre de la révision des Directives sur le blanchiment de capitaux en 1998, à l'occasion de l'intégration des nouvelles exigences de la Loi sur le blanchiment. Les affaires Abacha et Montesinos ont constitué des cas d'application récents de ces règles et, en particulier, de l'exigence de clarifier avec soin l'arrière-plan économique et le but d'une relation d'affaire ainsi que l'éventuelle qualité de PEP du client et de consulter de manière active des sources d'information publiques³⁷.

La Commission des banques peut prononcer des mesures administratives à l'encontre des personnes responsables et par exemple interdire à celles-ci de reprendre des fonctions ou des responsabilités comparables dans le secteur bancaire. Dans l'hypothèse où elle constate la présence de défauts d'organisation dans le domaine «Legal & Compliance» auprès d'un établissement surveillé, elle ordonnera à celui-ci de remédier rapidement à ces défauts, tout en maintenant un contrôle prudentiel serré. En cas de violations et de défauts d'organisation répétés, l'autorisation peut être retirée. Dans le cadre des dernières af-

³³ ATF 111 Ib 126.

³⁴ Art. 3 al. 2 lit. c LB.

³⁵ Rapport de gestion CFB 1987, p. 156.

³⁶ Rapport de gestion CFB 1997, p. 187 ss.

³⁷ Cf. Rapport de la CFB «Fonds «Abacha» auprès des banques suisses» du 30 août 2000, publié sur le site internet de la CFB (<http://www.ebk.admin.ch/ff/archiv/2000/neu14a-00.pdf>) ainsi que le communiqué de presse du 13 novembre 2001 dans l'affaire Montesinos (<http://www.ebk.admin.ch/ff/archiv/2001/neu1113-01f.pdf>).

faibles survenues, la Commission des banques a en outre informé le public du résultat de ses enquêtes et des mesures prises.

3.4 Autorégulation des banques

L'identification des clients des banques est réglée depuis 1977 déjà par les banques elles-mêmes dans leur Convention de diligence³⁸ révisée à plusieurs reprises. Dans le cadre de la législation pour la lutte contre le blanchiment, la Convention de diligence a en outre repris la fonction de concrétiser les devoirs de diligence en application de l'art. 16 LBA. La tâche de la Commission des banques en tant qu'autorité de surveillance instituée par une loi spéciale est de contrôler que la Convention de diligence règle de manière suffisante l'exécution des obligations découlant de la Loi sur le blanchiment. Les réviseurs externes sont pour leur part chargés de contrôler le respect de la Convention de diligence. Par ailleurs, une Commission de surveillance élue pour cinq ans par l'ASB veille à l'observation des dispositions conventionnelles. Elle prend ses décisions sur la base des réquisitions du chargé d'enquête qui est désigné par l'ASB également. Là où elle constate l'existence de violations des règles conventionnelles, elle peut prononcer des peines conventionnelles. La Commission de surveillance publie régulièrement un rapport d'activité donnant un aperçu de sa pratique³⁹.

Parallèlement à la refonte de la réglementation en matière de blanchiment, la CDB datant de 1998 a fait l'objet d'une révision⁴⁰. Cette sixième version (CDB 03) entre en vigueur le 1^{er} juillet 2003.

³⁸ Disponible sur l'internet sous http://www.swissbanking.org/110_f.pdf.

³⁹ «Aperçu de la jurisprudence pour la période 1998–2001», disponible sur l'internet: <http://www.swissbanking.org/fr/medienmitteilungen-40302.htm>.

⁴⁰ Cf. ch. 6 infra.

4 Développements internationaux

Ces dernières années, plusieurs groupes de travail internationaux ont développé des standards dans le domaine de la lutte contre le blanchiment. Les attentats terroristes du 11 septembre 2001 aux Etats-Unis ont conduit à un nouvel élargissement de la lutte contre le blanchiment et à l'adoption de recommandations en matière de lutte contre le financement du terrorisme. L'observation des standards minimaux internationaux fait maintenant l'objet de contrôles réguliers par des experts internationaux dans le cadre des examens auxquels sont soumis les pays, tels les processus d'évaluation mutuelle du GAFI⁴¹ ou le Financial Assessment Program du Fonds Monétaire International⁴². Il est en conséquence important de tenir compte des conditions-cadres internationales lors de révisions de la réglementation nationale en matière de lutte contre le blanchiment ou contre le financement du terrorisme. Les principaux instruments de réglementation internationaux sont passés en revue ci-après.

4.1 Les 40 Recommandations du GAFI (juin 1996)

Les 40 Recommandations du GAFI du 7 février 1990, modifiées le 28 juin 1996⁴³, constituent aujourd'hui des standards internationaux reconnus en matière de mesures à prendre par un pays pour combattre efficacement le blanchiment. Les Recommandations définissent des exigences minimales pour l'identification de clients et la conservation de la documentation, un devoir de diligence accru en cas de constatation et de communication de transactions suspectes ainsi que des mesures applicables aux relations avec des pays n'ayant pas pris de dis-

⁴¹ Le GAFI est un comité international indépendant dont le secrétariat est situé dans les locaux de l'OCDE. Les 29 pays membres du GAFI sont: l'Argentine, l'Autriche, la Belgique, le Brésil, le Canada, le Danemark, la Finlande, la France, l'Allemagne, la Grèce, Hong Kong, la Chine, l'Islande, l'Irlande, l'Italie, le Japon, le Luxembourg, le Mexique, les Pays-Bas, la Nouvelle-Zélande, la Norvège, le Portugal, Singapour, l'Espagne, la Suède, la Suisse, la Turquie, la Grande-Bretagne et les USA. Deux organisations internationales sont également membres du GAFI: l'Union Européenne et le Conseil de coopération du Golfe.

⁴² Cf. ch. 4.8. infra.

⁴³ Cf. Bulletin CFB 31, p. 19 ss; cf. également http://www.fatf-gafi.org/40Recs_fr.htm.

positions suffisantes pour lutter contre le blanchiment. Une version révisée des Recommandations devrait être adoptée d'ici juillet 2003. Un document consultatif a été publié en mai 2002⁴⁴.

En s'inspirant des Recommandations du GAFI, le Fonds Monétaire International et la Banque Mondiale ont développé une méthodologie⁴⁵ qui formule des critères pour l'évaluation du respect et de la mise en œuvre des dispositions pertinentes en matière de blanchiment, en particulier les Recommandations du GAFI. Cette méthodologie a pour but d'aider les examinateurs lors d'évaluations effectuées par le FMI, la Banque Mondiale et le GAFI à porter un jugement sur les systèmes anti-blanchiment des différents pays.

4.2 Recommandations du GAFI sur le financement du terrorisme (octobre 2001)

Lors de sa séance plénière extraordinaire d'octobre 2001 à Washington, le GAFI a adopté un programme immédiat aux termes duquel tous les pays du monde sont tenus de respecter sans délai les nouvelles Recommandations spéciales sur le financement du terrorisme⁴⁶. Ces recommandations prévoient notamment que tous les Etats étendent au financement du terrorisme le devoir d'effectuer des dénonciations de soupçons, qu'ils mettent en œuvre des obligations d'identification du client dans le cadre de transferts de fonds internationaux (Wire Transfers) et qu'ils veillent à ce que les entreprises, en particulier les associations de bienfaisance, ne soient pas utilisées pour le financement du terrorisme⁴⁷.

⁴⁴ Disponible sur l'internet: http://www.fatf-gafi.org/pdf/Review40_en.pdf.

⁴⁵ Fund and Bank Methodology for Assessing Legal, Institutional and Supervisory Aspects of Anti-Money Laundering and Combating the Financing of Terrorism (AML/CFT Methodology) 2002.

⁴⁶ Les Recommandations Spéciales sur le financement du terrorisme du 31 octobre 2001, disponibles sur l'internet: http://www.fatf-gafi.org/SRecsTF_fr.htm.

⁴⁷ Le GAFI a publié des directives devant aider dans la détection de liens avec des organisations terroristes ou avec le financement du terrorisme («Directives à l'attention des institutions financières pour la détection des activités de financement du terrorisme»), disponible sur l'internet: http://www1.oecd.org/fatf/pdf/GuidFITF01_fr.pdf.

4.3 Convention pour la répression du financement du terrorisme (décembre 1999)

La ratification et la mise en œuvre de la Convention internationale sur la répression du financement du terrorisme du 9 décembre 1999⁴⁸ constitue l'objet de l'une des Recommandations spéciales du GAFI en matière de lutte contre le financement du terrorisme. La convention en question définit le financement du terrorisme comme un délit autonome. L'acte est réprimé indépendamment du fait qu'un acte terroriste soit ou non réalisé. En outre, la convention contient des dispositions tendant à faciliter la coopération internationale et à empêcher la préparation et l'exécution d'activités financières soutenant le terrorisme. Le Conseil fédéral a décidé en novembre 2001 de ratifier la Convention pour la répression du financement du terrorisme et a transmis son Message y relatif au Parlement le 26 juin 2002⁴⁹. La norme sur le financement du terrorisme est au cœur de la révision du droit pénal. De plus, le champ d'application de la nouvelle disposition sur la responsabilité des entreprises, introduite dans le cadre de la révision de la partie générale du Code pénal de décembre 2002, devrait être étendu aux nouvelles infractions relatives au terrorisme.

4.4 Principes de Wolfsberg (2000/2002)

En octobre 2000, un groupe de banques d'importance mondiale s'est entendu sur des directives globales de lutte contre le blanchiment destinées à des banques privées actives au niveau international. Les principes dégagés s'intéressent à divers aspects des exigences du «Know Your Customer» dans les rapports entre des clients privés importants et les services Private Banking des instituts bancaires ainsi qu'à la détection et à l'observation d'activités inhabituelles ou suspectes. En janvier 2002, le groupe des banques du Forum de Wolfsberg a décidé d'étendre ses principes à la lutte contre le financement du terrorisme⁵⁰.

⁴⁸ International Convention for the Suppression of the Financing of Terrorism A/RES/54/109 <http://untreaty.un.org/French/Terrorism/Conv12.pdf>.

⁴⁹ Message disponible sur l'internet: <http://www.bk.admin.ch/ch/ff/ff/2002/5014.pdf>.

⁵⁰ Wolfsberg Statement on the suppression of the financing of terrorism, janvier 2002, disponible sur l'internet: <http://www.wolfsberg-principles.com>.

En mai 2002, les principes de Wolfsberg relatifs à la lutte contre le blanchiment ont été révisés⁵¹ et précisés sur certains points. En novembre 2002, des principes en matière de devoirs de diligence applicables en matière de correspondent banking ont été adoptés⁵². Ces derniers principes, de même que ceux publiés initialement en matière de lutte contre le blanchiment, reposent sur une approche différenciée en fonction des risques.

4.5 «Customer Due Diligence Paper» du Comité de Bâle (octobre 2001)

A fin 2001, le Comité de Bâle⁵³ a adopté les standards minimaux en matière d'identification de clients qui avaient été formulés par un groupe de travail composé de représentants du Comité de Bâle et du Groupe des organismes de supervision bancaire offshore. Ce document formule les nouveaux standards internationaux en matière de devoirs de diligence des banques et complète les Principes fondamentaux pour un contrôle bancaire efficace de septembre 1997 (en particulier le principe 15 concernant l'identification du client)⁵⁴. Comme toutes les autres publications du Comité de Bâle, ce texte n'a pas de force contraignante. Il constitue néanmoins un nouveau standard minimal au sujet duquel tous les membres du comité se sont déclarés en accord. Les standards minimaux exigent des groupes bancaires actifs sur un plan international qu'ils consolident au niveau du groupe leurs procédures d'identification de la clientèle ainsi que la gestion de leurs risques. De tels groupes sont tenus de déterminer, limiter et contrôler leurs risques juridiques et de réputation d'une manière globale. Suite aux événements du 11 septembre 2001, ce principe gagna encore en importance. Lors d'une conférence d'experts juridiques du groupe du G10 ayant pour objet un échange d'informations concernant la lutte

⁵¹ Disponible sur l'internet (http://www.wolfsberg-principles.com/wolfsberg_principles_1st_revision.html).

⁵² Disponible sur l'internet: http://www.wolfsberg-principles.com/wolfsberg_principles_correspondent.html.

⁵³ Le Comité de Bâle sur le contrôle bancaire a été créé en 1974 par les gouverneurs des banques centrales du G-10, auprès de la Banque des Règlements Internationaux (BRI) à Bâle. Le comité se compose de représentants des banques centrales et autorités de surveillance bancaires des treize pays suivants: Belgique, Allemagne, France, Italie, Japon, Canada, Luxembourg, Pays-Bas, Suède, Suisse, Espagne, Grande-Bretagne et USA.

⁵⁴ Customer due diligence for banks (<http://bis.org/publ/bcb85.htm>); Principes fondamentaux pour un contrôle bancaire efficace, publiés dans le Bulletin CFB 33, p. 141 ss.

contre le financement du terrorisme, fut soulignée dans un document commun d'une part la nécessité d'une coopération plus étroite entre les autorités de surveillance et d'autre part l'exigence d'un système de gestion des risques centralisé pour les groupes bancaires internationaux⁵⁵.

4.6 «Supervisors' PEP working paper 2001» (novembre 2001)

En novembre 2000 a eu lieu à Lausanne, à l'initiative de la Suisse, une conférence sur le traitement des relations avec des PEP. Des représentants des organes de la justice et des autorités de surveillance bancaires des membres du G-7 ainsi que de la Suisse ont procédé à une réflexion sur la question des PEP et discuté les conclusions tirées dans le cadre de l'affaire Abacha. Les recommandations élaborées à l'issue de cette rencontre par des représentants des autorités de surveillance des pays du G-7 et de la Suisse concernant l'acceptation de valeurs patrimoniales de personnes occupant des fonctions officielles importantes ont été mises au point en novembre 2001⁵⁶. Le document pose les bases d'une réglementation des relations d'affaires avec des personnes occupant des fonctions officielles importantes, qui correspond aux propositions retenues dans l'Ordonnance.

⁵⁵ Sharing of financial records between jurisdictions in connection with the fight against terrorist financing, Summary of a meeting of representatives of Supervisors and Legal Experts of G10 Central Banks and Supervisory Authorities on 14 December 2001, Basel, Switzerland, disponible sur le site internet de la BRI: <http://www.bis.org/publ/bcbs89.pdf>.

⁵⁶ Supervisor's PEP working paper 2001, disponible sur le site internet de la CFB: <http://www.ebk.admin.ch/f/aktuell/neu090702-03f.pdf>.

⁵⁷ Directive 91/308/CEE du Conseil (Journal Officiel L 166 du 10 juin 1991, p. 77 ss), relative à la prévention de l'utilisation du système financier aux fins du blanchiment de capitaux, et Directive 2001/97/CE du Parlement européen et du Conseil modifiant la Directive 91/308/CEE du Conseil relative à la prévention de l'utilisation du système financier aux fins du blanchiment de capitaux (Journal Officiel L 344 du 28 décembre 2001, p. 76 ss). La modification de la Directive sur le blanchiment de capitaux (91/308/CEE) a notamment comporté un élargissement de la notion de blanchiment à tous les revenus résultant de délits graves, l'ancienne version ne s'appliquait qu'aux revenus provenant d'infractions à la législation relative aux stupéfiants. De surcroît, la nouvelle directive étend le champ d'application de l'ancienne directive (limitée au secteur financier) à une série d'activités du secteur non financier et de professions pouvant facilement être instrumentalisées pour le blanchiment, soit les agents immobiliers, les notaires, les avocats, les marchands d'art, les commissaires priseurs et les casinos.

4.7 Autres instruments internationaux d'importance

Au titre d'instruments internationaux importants peuvent également être mentionnés la Directive européenne du 10 juin 1991 sur le blanchiment (élargie par la Directive 2001/97 du 4 décembre 2001)⁵⁷, le Deuxième Protocole à la Convention relative à la protection des intérêts financiers des Communautés européennes⁵⁸, la Décision-Cadre du Conseil du 26 juin 2001 concernant le blanchiment d'argent, l'identification, le dépistage, le gel ou la saisie et la confiscation des instruments et des produits du crime⁵⁹, la Convention de Vienne des Nations Unies relative au trafic illicite des substances narcotiques du 19 décembre 1988⁶⁰, la Convention du Conseil de l'Europe du 8 novembre 1990 relative au blanchiment, au dépistage, à la saisie et à la confiscation des produits du crime⁶¹, la Convention de l'OCDE sur la lutte contre la Corruption d'agents publics étrangers dans les transactions commerciales internationales du 21 novembre 1997⁶², la Convention pénale sur la corruption du 27 janvier 1999⁶³ ainsi que la Convention des Nations Unies contre la criminalité transnationale organisée⁶⁴ publiée en 2000.

4.8 FMI – Financial Sector Assessment Switzerland (juin 2002)

Durant l'année 2001, le Fonds Monétaire International a réalisé en Suisse une évaluation du secteur financier national (Financial Sector Assessment Program)⁶⁵. Au moyen de questionnaires standardisés, le FMI a contrôlé l'observation des standards et réglementations recon-

⁵⁸ Journal Officiel C 221 du 19 juillet 1997, p. 12 ss.

⁵⁹ Journal Officiel L 182 du 5.7.2001, p. 1, disponible sur l'internet:

http://www.europa.eu.int/servlet/portail/RenderServlet?search=RefPub&lg=fr&nb_docs=25&domain=&in_force=NO&year=2001&month=7&day=5&coll=JOL&nu_jo=182&page=1.

⁶⁰ United Nations Convention against illicit traffic in narcotic drugs and psychotropic substances, disponible sur l'internet: http://www.incb.org/e/ind_conv.htm.

⁶¹ Disponible sur l'internet: <http://conventions.coe.int/treaty/FR/Treaties/Html/141.htm>. La Convention a été signée par la Suisse le 11 mai 1993.

⁶² Disponible sur l'internet: <http://www.admin.ch/ch/f/ff/1999/5108.pdf>. La Convention a été ratifiée le 21 mai 2000 par la Suisse.

⁶³ Disponible sur l'internet: <http://conventions.coe.int/Treaty/FR/CadreListeTraites.htm>.

⁶⁴ Disponible sur l'internet:

http://www.uncjin.org/Documents/Conventions/dcatoc/final_documents_2/convention_french.pdf.

⁶⁵ Cf. Rapport de gestion CFB 2001, p. 162 ss; Rapport de gestion CFB 2000, p. 174 s.

nus au niveau international dans les domaines de la surveillance des banques, des bourses, des marchés, des assurances et des systèmes de paiement ainsi qu'en ce qui concerne les questions de transparence en matière de politique monétaire et financière. Bien que le but de l'exercice soit en premier lieu l'analyse et le renforcement de la stabilité du système financier sur un plan national et international, le domaine de la lutte contre le blanchiment fait également partie du champ d'évaluation. Le FMI a développé une méthodologie devant servir dans le cadre de ses évaluations qui résume les standards de surveillance internationaux pertinents en matière de blanchiment. Les travaux d'élaboration de cette méthodologie n'étant pas terminés au moment de l'évaluation de la Suisse, celle-ci s'est déclarée prête à procéder à une première utilisation pilote du projet dans le cadre du Financial Assessment Program. Les dispositions suisses de lutte contre le blanchiment applicables au secteur bancaire ont été jugées appropriées et en accord avec les standards internationaux. Le FMI s'est prononcé de manière différenciée pour ce qui est des négociants en valeurs mobilières, bien que les règles applicables à ceux-ci soient fondamentalement identiques à celles applicables aux banques. Le fait qu'il ne soit pas procédé à l'identification de l'ayant droit économique de manière systématique a par exemple été critiqué. Un rapport résumé du Financial Assessment Program de la Suisse a été publié en juin 2002⁶⁶.

5 Grandes lignes de l'Ordonnance

5.1 Ordonnance en remplacement des Directives de la CFB sur le blanchiment de capitaux

Depuis l'entrée en vigueur de la Loi sur le blanchiment au 1^{er} avril 1998, les art. 16 al. 1 et 41 LBA constituent une base légale expresse permettant à la CFB d'émettre une ordonnance réglant le domaine. La réglementation en matière de blanchiment acquerra un poids majeur par le fait qu'elle est arrêtée sous forme d'ordonnance. D'un point de

⁶⁶ Ce rapport peut être consulté sur le site internet du FMI:
<http://www.imf.org/external/pubs/ft/ser/2002/cr02108.pdf>.

vue de technique législative, une ordonnance de la CFB se distingue d'une circulaire par son applicabilité directe. Une circulaire représente une aide à l'interprétation et ne déploie par conséquent, au contraire d'une ordonnance qui est publiée dans le Recueil officiel du droit fédéral, aucun effet de droit matériel. De facto, une circulaire et une ordonnance revêtent cependant le même caractère obligatoire. Le choix de l'ordonnance nécessite toutefois l'usage d'un langage plus condensé, de sorte qu'il en résulte une réglementation sensiblement plus courte, malgré l'intégration de la réglementation sur le commerce professionnel de billets de banque ainsi que d'une série de dispositions additionnelles, telles celles sur la lutte contre le financement du terrorisme. Cette technique de réglementation correspond également à celle de l'Autorité de contrôle qui a elle aussi réglé les devoirs de diligence des intermédiaires financiers qui lui sont directement soumis dans une ordonnance. L'ordonnance sur le blanchiment d'argent de la CFB constitue un complément à la loi sur le blanchiment et ne répète en conséquence aucune disposition contenue dans celle-ci.

5.2 Délimitation matérielle par rapport à l'autorégulation

Les Directives sur le blanchiment de capitaux ne contiennent aujourd'hui aucune règle en matière de vérification de l'identité du cocontractant et d'identification de l'ayant droit économique lors de l'ouverture de compte. Ces prescriptions, formelles et plus détaillées, devant concrétiser les art. 3–5 de la loi sur le blanchiment sont contenues dans la Convention de diligence de l'ASB, laquelle a fait l'objet de sa sixième révision depuis 1977 en décembre 2002. La CFB a reconnu à cette autorégulation le caractère de standard minimum valable pour toutes les banques et les négociants en valeurs mobilières⁶⁷. Les Directives sur le blanchiment de capitaux actuelles règlent pour leur part les mesures de nature organisationnelle en vue de prévenir le blanchiment d'argent (art. 7 et 8 LBA), elles donnent des indications concernant le comportement à observer lors de transactions ou relations d'affaires inhabituelles (art. 6 LBA) et précisent les devoirs en cas

⁶⁷ Circ.-CFB 96/3, annexe I.

de soupçons de blanchiment (art. 9 et 10 LBA). En comparaison avec la Convention de diligence, la réglementation de la CFB est rédigée de manière plus générale.

La CFB considère toujours ce système comme adéquat. Sans cette distinction matérielle, il en résulterait des chevauchements supplémentaires au sein de la structure normative déjà complexe qui est celle de la lutte contre le blanchiment. Par ailleurs, aux termes de la loi sur le blanchiment, la CFB doit tenir compte de l'autorégulation (art. 16 al. 1 LBA). Le fait que l'Ordonnance présente un degré de détails inférieur en comparaison avec la Convention de diligence est justifié au vu de la diversité des entreprises assujetties à la surveillance de la CFB. Cette diversité exige en effet une certaine flexibilité dans la mise en œuvre de la réglementation anti-blanchiment. Le concept de mise en œuvre de chacun des intermédiaires financiers doit être adapté aux risques spécifiques encourus par ceux-ci, à leur taille, au cercle de leur clientèle ainsi qu'aux types de prestations qu'ils offrent. Les exigences de l'Ordonnance ne seront effectives qu'après avoir été concrétisées dans les directives internes et les manuels de «Compliance» des intermédiaires financiers.

5.3 Développement des règles sur les personnes politiquement exposées

En 1998, suite à l'affaire Mobutu et à l'occasion d'une révision de sa circulaire de 1991, la CFB décida de manière intentionnelle d'inscrire et en partie de préciser les règles développées en matière de traitement des relations d'affaires avec des PEP. Cette réglementation a fait ses preuves. En grande partie en raison de la publicité autour de l'affaire Abacha et sur l'initiative de la Suisse, la problématique fut ensuite abordée au niveau international⁶⁸. Le risque de réputation lié à l'acceptation de fonds issus de la corruption s'est encore accru avec l'attention majeure portée à la question par les instances internatio-

⁶⁸ Voir «Supervisors' PEP Working Paper 2001», annexe II du Rapport du Groupe de travail KYC, juin 2002, disponible sur l'internet sous <http://www.ebk.admin.ch/f/archiv/2002/neu090702-03d.pdf>.

nales et les médias. Finalement, l'acceptation et la gestion de fonds issus de la corruption ne portent pas uniquement atteinte à la réputation de l'établissement concerné, mais également à la confiance du public dans les standards éthiques appliqués par la place financière dans son ensemble.

Les procédures de la CFB dans les affaires Abacha et Montesinos firent ressortir des points faibles en matière de clarification de relations d'affaires inhabituelles auprès des établissements concernés, ce qui incita la CFB à exiger un renforcement des devoirs de diligence applicables aux relations d'affaires avec des PEPs. La nouvelle Ordonnance confère aux règles relatives au traitement des relations avec des PEPs une visibilité accrue. Des devoirs de clarification et de contrôle complémentaires sont maintenant expressément applicables à ce type de relations, de même qu'aux relations avec des personnes qui sont jugées par l'intermédiaire financier comme comportant des risques accrus. La décision de l'admission ou de la poursuite de relations d'affaires avec des personnes politiquement exposées relève, comme cela était le cas jusqu'à aujourd'hui, de la direction à son plus haut niveau ou de l'un au moins des membres de celle-ci.

5.4 Devoir de diligence différencié en fonction des risques

L'Ordonnance exige, au contraire des obligations d'identification découlant de la CDB et applicables uniformément à toutes les relations d'affaires, l'application d'un devoir de diligence accru aux relations présentant de manière abstraite des risques accrus. Cette nouvelle exigence ne s'applique donc pas à l'ensemble de la clientèle et, à l'opposé, ne se limite pas aux relations avec les PEPs.

Les clients présentent de manière abstraite des risques accrus en fonction notamment de leur lieu de domicile, de leur activité professionnelle ou du type de transactions qu'ils effectuent. Les intermédiaires

financiers doivent définir les critères qu'ils considèrent comme pertinents sur la base des indices énumérés de manière exemplative dans l'Ordonnance. Cela présuppose qu'ils avaient auparavant analysé les risques spécifiques liés à leur activité et au cercle de leur clientèle. L'Ordonnance renonce à établir une liste exhaustive des critères de risques, permettant ainsi aux intermédiaires financiers de choisir les critères les plus adaptés à leur domaine d'activité. Les relations d'affaires comportant des risques accrus devront faire l'objet de clarifications approfondies. Il y aura lieu de consulter à cet effet différentes sources. En outre, la direction à son plus haut niveau devra être impliquée d'une manière plus directe et plus systématique que jusqu'à maintenant dans le processus de contrôle de ces relations d'affaires.

Le concept de surveillance et de contrôle différenciés en fonction du risque n'est pas nouveau. Il est à la base des contrôles de tous les types de risques, de manière plus traditionnelle des risques de marchés et de crédit, et suppose une analyse préalable approfondie des risques. L'intermédiaire financier peut être exposé à d'importants risques par suite de négligence lors de l'établissement et de la surveillance de relations d'affaires, notamment des risques juridiques et des risques de réputation ainsi que des risques opérationnels ou de concentration⁶⁹. D'importantes conséquences financières peuvent résulter pour l'intermédiaire financier de prétentions dirigées à son encontre, de saisies ou de blocages de valeurs patrimoniales ainsi que de défaillances de crédits.

5.5 Surveillance systématisée des transactions

Une des nouveautés de l'Ordonnance est l'introduction d'une obligation de surveiller les transactions de manière systématisée. La surveillance continue des transactions constitue une composante essentielle de la prévention du blanchiment d'argent. A cet effet, l'inter-

⁶⁹ Cf. Customer Due Diligence, note 54, ch. 10–15.

médiaire financier devra se servir d'un système informatique⁷⁰. Celle-ci offre en effet des possibilités très étendues de surveillance automatique des transactions. L'étendue de la surveillance informatisée doit être adaptée aux risques. Un intermédiaire financier doit disposer d'un système qui l'aide à détecter des procédés inhabituels ou suspects sur l'ensemble de ses comptes. Cela peut en particulier se faire par la fixation de limites pour un groupe déterminé ou une catégorie déterminée de comptes. La plausibilité des transactions filtrées par le système doit ensuite être contrôlées manuellement. Ici également, l'Ordonnance vise une approche différenciée en fonction du risque spécifique auquel est exposé un intermédiaire financier. Il reviendra fondamentalement à celui-ci de déterminer les paramètres pertinents pour sa surveillance des transactions. Les exigences mentionnées dans l'Ordonnance ne constituent en conséquence pas de standards minimaux à observer par l'ensemble des intermédiaires financiers⁷¹.

La CFB est d'avis que l'usage de la technologie informatique devrait permettre une surveillance des transactions plus efficace et exige donc en principe l'introduction d'un système informatisé qui tienne compte des particularités de l'établissement concerné. Les plus petites structures seront toutefois autorisées, à certaines conditions, à procéder à une surveillance manuelle.

5.6 E-Banking

La CFB est convaincue que l'usage de l'internet ne modifie pas fondamentalement les relations entre la banque et ses clients. Les ouvertures de compte par voie purement électronique ne constituent en réalité rien moins qu'une espèce de relations «non face to face». D'une

⁷⁰ Le marché propose en gros trois types de modèles informatiques pour détecter des transactions suspectes: les systèmes se bornant à filtrer les transactions en fonction de critères fixes préétablis («business rules approach»), ceux qui se fondent sur des données statistiques pour établir différents segments de risque à l'intérieur d'une structure («statistical profiling») et enfin ceux qui utilisent l'intelligence artificielle. Les systèmes les plus sophistiqués sont naturellement ceux qui combinent ces différentes techniques.

⁷¹ Le système doit cependant être en mesure de détecter dans tous les cas des transactions au comptant d'une valeur de plus de CHF 100 000, art. 8 al. 3 lit. a et art. 12 al. 1 OBA-CFB.

manière générale, les risques sont les mêmes selon qu'une transaction est effectuée par le biais de l'internet ou en utilisant des canaux traditionnels. Les prescriptions relatives au traitement des relations et transactions présentant des risques accrus et en particulier l'exigence d'un système de surveillance des transactions informatisé constituent pour la CFB des mesures adéquates pour les banques électroniques. Aucune règle spéciale n'est par conséquent nécessaire. Les Standards minimaux applicables aux banques et négociants actifs sur l'internet exclusivement adoptés par la CFB le 29 mars 2001 rendent obligatoire, lors de l'ouverture de comptes par des clients importants, une rencontre avec ceux-ci. De manière identique, une rencontre de l'ayant droit économique des sociétés de domicile est exigée selon les mêmes critères que ceux valables pour l'ouverture de compte par des personnes physiques. L'Ordonnance considère l'absence de rencontre avec le cocontractant ainsi qu'avec l'ayant droit économique comme un critère entraînant la qualification d'une relation d'affaires comme comportant des risques plus élevés. Le risque potentiellement plus élevé résultant de l'absence de rencontre avec le client doit, en particulier dans le cas de banques électroniques pures, être compensé dans le cadre de la constitution de catégories de risques ainsi que par la mise en place de systèmes de surveillance des transactions et par la fixation de limites plus basses. Au sens de la CFB, l'Ordonnance tient compte des points essentiels des Standards minimaux.

5.7 Gestion globale des risques de réputation

Les risques juridiques et les risques de réputation, de même que les autres types de risques de l'activité bancaire, ne connaissent pas de frontière. La prévention du blanchiment ne peut donner des résultats que si elle s'applique à l'ensemble d'un groupe. La détermination, la limitation et le contrôle des risques juridiques et des risques de réputation résultant de certaines relations d'affaires ne peuvent avoir lieu d'une manière efficace que sur une base consolidée. Les Directives sur

le blanchiment des capitaux interdisent aux intermédiaires financiers d'utiliser leurs succursales ou d'autres sociétés du groupe à l'étranger, actives dans le domaine de la finance, pour contourner ces directives⁷². L'Ordonnance précise cette interdiction en prescrivant une application des principes fondamentaux de l'Ordonnance aux succursales et sociétés du groupe de l'intermédiaire financier à l'étranger.

En outre, les groupes financiers internationaux qui ont leur siège en Suisse sont tenus de déterminer, limiter et contrôler d'une manière globale leurs risques juridiques et de réputation résultant du blanchiment et du financement du terrorisme. A cette fin, l'organe de contrôle interne ainsi que les réviseurs externes du groupe doivent avoir accès aux informations sur les cocontractants et sur les ayants droit économiques de relations d'affaires de l'ensemble du groupe. La constitution d'une banque de donnée centrale contenant le nom de l'ensemble de la clientèle n'est pas exigée des groupes financiers suisses et n'est pas permise en ce qui concerne la clientèle des filiales suisses de groupes étrangers. Les intermédiaires financiers sis en Suisse faisant partie d'un groupe suisse ou international doivent toutefois permettre l'accès des organes de contrôle du groupe aux informations concernant leurs relations d'affaires, dans la mesure nécessaire pour la gestion globale des risques de réputation. Ces nouvelles exigences correspondent aux derniers développements des standards internationaux⁷³.

5.8 Lutte contre le financement du terrorisme

Suite aux événements du 11 septembre 2001, la lutte contre le financement du terrorisme se hissa au rang des priorités internationales. Dès lors que les organisations terroristes ont besoin pour leur financement des systèmes de paiements bancaires, les normes anti-blanchiment devraient être utilisées de manière accrue également dans la lutte contre le financement du terrorisme. Les initiatives prises par les

⁷² Ch. 6 Circ.-CFB 98/1.

⁷³ Cf. Customer Due Diligence, ch. 63 ss, en particulier note 54.

Etats-Unis dans le cadre de la recherche des fonds terroristes de même que l'adoption des huit Recommandations spéciales du GAFI sur le financement du terrorisme accentuent la pression exercée sur les législations nationales pour la mise en place des mesures normatives nécessaires. Un élargissement correspondant du champ d'application de l'Ordonnance s'est par conséquent révélé indispensable.

6 Convention de diligence

La question de l'identification par les banques de leurs partenaires contractuels et des ayants droit économiques est un point central de la lutte contre le blanchiment dont le détail restera réglé à l'avenir également par la Convention de diligence.

La Convention de diligence révisée a été adoptée par le Conseil d'administration de l'Association suisse des banquiers le 2 décembre 2002, après concertation avec la CFB. Le catalogue des points à examiner dans le cadre de la révision de la Convention de diligence, catalogue établi par le Groupe de travail KYC⁷⁴, a été largement pris en compte. Son entrée en vigueur a été fixée au 1^{er} juillet 2003, soit simultanément à l'entrée en vigueur de l'Ordonnance.

Quelques-unes des principales modifications apportées au texte de la Convention du 28 janvier 1998 sont décrites ci-après⁷⁵:

- Le préambule complète le but de la CDB en y ajoutant la lutte contre le financement du terrorisme.
- Il est expressément mentionné que les devoirs de clarification spéciaux en cas de relation d'affaires inhabituelle sont réglés par l'Ordonnance sur le blanchiment de la CFB (et que, par conséquent, une

⁷⁴ Annexe II au Rapport du Groupe de travail KYC, cf. note 1 supra.

⁷⁵ Des indications supplémentaires relatives aux nouveautés introduites dans la CDB figurent sur le site internet de l'ASB <http://www.sba.ch>.

violation de ceux-ci ne peut faire l'objet d'une sanction par la Commission de surveillance CDB).

- Le régime spécial d'identification pour les personnes connues personnellement est supprimé. Seules demeurent admises les pièces de légitimation officielles comportant une photographie.
- L'envoi postal à des fins d'identification est supprimé. Il est toutefois maintenu pour permettre une vérification de l'adresse.
- L'exception qui concernait les comptes de mineurs est supprimée. Est exigée une identification de la personne majeure qui ouvre le compte pour le mineur.
- Dans des cas exceptionnels, la CDB accorde un délai de grâce de 30 jours pour compléter une documentation d'ouverture de compte incomplète. Des retraits à la demande du client ne sont pas autorisés pendant ce délai.
- La CDB contient une nouvelle réglementation en matière de délégation de l'identification qui se calque sur celle prévue par l'Ordonnance pour la délégation des clarifications complémentaires. La banque est autorisée à déléguer l'identification sur la base d'une convention écrite à des personnes ou entreprises, dans la mesure où elle a instruit ceux-ci et où elle est en mesure de contrôler si l'identification a été effectuée de manière correcte. Le mandataire doit transmettre à la banque les documents sur lesquels repose l'identification. Une sous-délégation par le mandataire est exclue.
- Les indications devant obligatoirement figurer dans le formulaire A ont été étendues à la date de naissance et à la nationalité de l'ayant droit économique.
- La réglementation souligne le fait qu'il faille toujours se demander si le cocontractant est bien lui-même l'ayant droit économique.
- Des devoirs de diligence supplémentaires sont requis concernant les associations de bienfaisance («charities»), soit en particulier pour les associations et les fondations. Les banques sont tenues d'identifier la personne qui requiert l'ouverture du compte dans la mesure où elle possède le droit de signature.

- Les associations de bienfaisance ne sont plus exemptées de manière systématique de la procédure d'identification de l'ayant droit économique. Il s'agit là d'une mise en œuvre des Recommandations Spéciales du GAFI sur le financement du terrorisme.
- La procédure d'ouverture de compte par correspondance, désormais applicable également aux établissements actifs exclusivement sur l'internet, a été précisée. Dans la mesure où la relation d'affaires est nouée par correspondance ou sur l'internet, la banque doit d'une part vérifier l'identité du cocontractant en se faisant remettre une copie certifiée d'une pièce de légitimation et d'autre part se faire confirmer l'adresse du domicile du cocontractant par l'établissement d'une correspondance ou par un autre moyen équivalent.
- Les banques établies dans des pays ne disposant pas de surveillance et de réglementation appropriées en matière de lutte contre le blanchiment doivent faire connaître l'ayant droit économique lorsqu'elles détiennent, auprès d'établissements suisses, des comptes comportant des sous-rubriques pour le compte de clients dont le nom n'est pas divulgué. Avec le terme «banques et autres intermédiaires financiers domiciliés à l'étranger, soumis à une surveillance et à une réglementation appropriées en matière de lutte contre le blanchiment», la CDB se réfère aux pays membres du GAFI⁷⁶.

7 Commentaire de l'Ordonnance

7.1 Dispositions générales

Art. 1 Définitions

La définition des *personnes politiquement exposées* (PEP, lit. a) a été laissée relativement ouverte en considération du fait que l'importance d'une fonction peut fortement varier d'un pays à l'autre (lit. a). De même que jusqu'à présent, le parti a été pris d'exclure de la définition

⁷⁶ Cf. liste des membres du GAFI, note 41 supra. Les banques ainsi que les autres intermédiaires domiciliés dans la Principauté de Liechtenstein sont assimilés aux intermédiaires correspondants des pays du GAFI dans le cadre de cette réglementation.

les PEP suisses, soit les personnes exerçant une fonction publique en Suisse⁷⁷. La solution contraire aurait fait sensiblement grossir le cercle des personnes concernées, ce qui aurait entraîné des difficultés pratiques, dans la mesure où la direction devrait prendre des décisions pour toutes les relations d'affaires avec des PEP suisses. Bien que ces dernières ne doivent pas être classées *ex lege*, au contraire de ce qui vaut pour les relations avec les PEP étrangers, dans le cercle des relations comportant des risques accrus, cela ne signifie pas pour autant qu'une banque ne puisse pas, dans un cas particulier, les désigner comme telles sur la base des critères de risques qu'elle a développés (art. 7 al. 2) ou sur la base de constatations faites dans le cadre de la surveillance des transactions. Dans un tel cas, le devoir de clarification serait absolument identique à celui applicable aux PEP étrangers. Un PEP qui quitte ses fonctions publiques ne conservera pas son statut de PEP pour une durée illimitée, dans la mesure où il n'est pas également proche d'un autre PEP par exemple.

L'Ordonnance intègre dans la mesure utile la réglementation contenue jusqu'à présent dans la Circulaire sur la réglementation du commerce professionnel des billets de banque⁷⁸. La définition du *Négociant professionnel* (lit. b) correspond en grande partie au contenu de celle qui prévaut actuellement qui a été simplifiée.

Dès lors que les modifications du Code pénal nécessaires en vue de la mise en œuvre de la Convention sur le financement du terrorisme ne sont pas encore définitives, la réglementation en vigueur ne connaît pas de définition du terrorisme ou du financement du terrorisme à laquelle il pourrait être fait référence. La CFB ne peut toutefois renoncer à l'utilisation de ces notions et de celle de *l'organisation terroriste* (lit. c) afin d'être en mesure de préciser les devoirs des intermédiaires financiers et de mettre en œuvre les recommandations internationa-

⁷⁷ Voir les Directives sur le blanchiment de capitaux de la CFB, de même que la nouvelle réglementation aux USA (Proposed Rules du US Treasury, p. 10 et 27, mise en œuvre du § 312 du Patriot Act, disponible sur l'internet: <http://www.treas.gov/press/releases/docs/nprm.pdf>).

⁷⁸ Voir <http://www.ebk.admin.ch/fi/publik/bulletin/bull20.pdf>; p. 101 (en version allemande uniquement).

les⁷⁹. Seront par conséquent considérées comme organisations terroristes les organisations criminelles au sens de l'art. 260^{ter} du Code pénal. Selon le Message, l'état de fait relatif aux organisations criminelles de l'art. 260^{ter} du Code pénal devait dès l'origine comprendre aussi bien les organisations mafieuses que celles terroristes⁸⁰. Il sera sans doute nécessaire d'adapter la définition suite à l'aboutissement de la réforme en cours du droit pénal.

Art. 2 Champ d'application

L'Ordonnance ne prévoit pas de modifications fondamentales par rapport au champ d'application des Directives sur le blanchiment de capitaux (al. 1).

Cette disposition reprend la possibilité offerte au ch. 5 Circ.-CFB 98/1 – et consentie en accord avec l'Autorité de contrôle – de soumettre à la surveillance de la CFB en matière de blanchiment les sociétés suisses faisant partie du même groupe d'une banque ou d'un négociant en valeurs mobilières dans la mesure où ces sociétés ne font pas l'objet d'une surveillance en vertu d'une loi spéciale⁸¹, mais qui exercent des activités financières au sens de l'art. 2 al. 3 LBA. Ce régime n'est toutefois consenti que sur requête et à condition que les exigences énumérées aux lettres a à e soient remplies. Il vaut explicitement pour les sociétés-sœurs de banques et négociants en valeurs mobilières. Le but de cet assujettissement est de permettre, pour les groupes suisses, un contrôle prudentiel de la gestion globale des risques juridiques et de réputation exigée par l'Ordonnance (art. 9) selon des standards uniformes.

Par les conditions posées à cet assujettissement ad hoc à l'alinéa 2, est visée une égalité de traitement des intermédiaires financiers bénéficiant du régime spécial de la présente disposition par rapport à ceux

⁷⁹ Voir supra ch. 4.2 et 4.3.

⁸⁰ Voir Message du 30 juin 1993, FF 1993 III 269 (287).

⁸¹ Conformément à l'art. 2 al. 2 LBA.

qui exercent une activité identique tout en étant assujettis à la surveillance de l'Autorité de contrôle. Du fait que la société requérante n'est pas soumise elle-même à la surveillance prudentielle de la CFB, elle doit reconnaître les pouvoirs prudentiels de la CFB (al. 2 lit. c). Par ailleurs, le groupe – qui est pour sa part soumis à la surveillance consolidée de la CFB – doit contrôler l'observation de l'Ordonnance par les sociétés de son groupe qu'il veut soumettre à la surveillance de la CFB (al. 2 lit. d). Cette dernière condition correspond à l'obligation d'une gestion globalisée des risques juridiques et de réputation au niveau du groupe⁸².

Le réviseur externe du groupe doit effectuer un contrôle pour chaque société du groupe bénéficiant du régime spécial de l'art. 2 al. 2. Il doit prendre position dans son rapport de manière individuelle pour chacune de ces sociétés relativement au respect des obligations qui ressortent de la Loi sur le blanchiment ainsi que de l'Ordonnance (art. 31), y compris de la Convention de diligence (art. 14 al. 1).

Art. 3 Succursales et sociétés de groupe à l'étranger

Cette disposition va un peu plus loin que les Directives sur le blanchiment de capitaux qui interdisent uniquement d'utiliser les succursales étrangères ou les sociétés du groupe à l'étranger pour les contourner⁸³. En conformité avec les recommandations contenues dans le Customer Due Diligence Paper⁸⁴, les principes fondamentaux de l'Ordonnance sont déclarés applicables également aux succursales et aux sociétés étrangères du groupe. Sont comprises les filiales et, cas échéant, les sociétés sœurs, qui font partie du périmètre de consolidation du groupe (art. 1 lit. d) lorsqu'elles sont actives dans le domaine de la finance.

Dans la mesure où une application des principes fondamentaux de l'Ordonnance devait entraîner un désavantage concurrentiel pour l'in-

⁸² Cf. art. 9 infra.

⁸³ Cf. ch. 6 Circ.-CFB 98/1.

⁸⁴ Cf. Customer Due Diligence, ch. 54; cf. également ch. 4.5 supra.

termédiaire financier, celui-ci pourrait en informer la CFB, de même que lorsque des prescriptions locales interdisent l'application de ces principes (al. 2). La CFB procédera à une évaluation de la situation et tentera de résoudre celle-ci avec le concours des autorités locales. En cas d'échec, différentes options s'offriront à la CFB en fonction des circonstances: la CFB pourra prononcer l'interdiction de s'implanter dans cette juridiction dans des cas extrêmes ou, à l'inverse, libérer le groupe de l'application de certains des principes de l'Ordonnance.

La communication des transactions ou relations suspectes et le blocage des avoirs s'effectueront dans tous les cas conformément aux dispositions locales (al. 3).

7.2 Principes

Art. 4 Interdiction de l'acceptation de valeurs patrimoniales provenant de la corruption et d'autres crimes

L'acceptation intentionnelle⁸⁵ de valeurs patrimoniales d'origine criminelle constitue un cas de blanchiment au sens de l'art. 305^{bis} CP, puisqu'elle réalise un acte potentiel d'entrave à l'identification de l'origine, à la découverte ou à la confiscation de valeurs patrimoniales (al. 1). Sont des crimes tous les actes passibles de réclusion⁸⁶ aux termes du droit suisse, y compris ceux commis à l'étranger⁸⁷. Le blanchiment par métier d'importantes sommes peut également constituer une infraction préalable au blanchiment⁸⁸.

L'alinéa 2 cite spécifiquement une série de crimes relevant de la corruption et du détournement de fonds publics. Cette précision n'est pas indispensable d'un point de vue juridique, mais peut être utile dans la mesure où l'acceptation de tels fonds s'est révélée être l'un des risques de réputation majeurs auxquels sont exposés les banques et la place financière, ainsi que l'ont démontré les affaires Abacha et Montesinos.

⁸⁵ Pour une définition de l'intention, voir art. 18 al. 2 CP.

⁸⁶ Art. 9 et 35 CP.

⁸⁷ Art. 305^{bis} ch. 3 CP.

⁸⁸ Art. 305^{bis} ch. 2 lit. c CP.

L'acceptation par négligence de valeurs patrimoniales provenant d'un crime n'est pas pénalement punissable. Toutefois, les intermédiaires financiers soumis à la surveillance de la CFB ne peuvent exercer leur activité qu'après l'octroi d'une autorisation⁸⁹. La délivrance (et le maintien) de celle-ci dépend de l'observation d'un certain nombre de conditions, au nombre desquelles figure la garantie d'une activité irréprochable⁹⁰. Dans la mesure où l'intermédiaire financier a accepté des valeurs patrimoniales provenant d'un crime par suite de négligence, on peut se demander si cette condition d'autorisation est toujours remplie (al. 3).

Art. 5 Interdiction de relations d'affaires avec des organisations criminelles ou terroristes

L'acceptation de valeurs patrimoniales d'organisations criminelles ou terroristes constitue également un acte de blanchiment d'argent. L'employé⁹¹ d'un intermédiaire financier qui y procéderait de manière intentionnelle pourrait se rendre lui-même coupable de soutien à une organisation criminelle.

Art. 6 Relations avec des banques correspondantes

Les comptes correspondants ouverts au nom de banques «clientes» sont soumis aux règles ordinaires de l'Ordonnance (al. 1), ce qui signifie que de telles relations peuvent aussi devoir être classées comme relations comportant des risques accrus.

Conformément aux recommandations internationales, les intermédiaires financiers ne devront plus entretenir de relations d'affaires avec des banques qui n'ont pas de présence physique au lieu de leur incorporation («shell banks»), autrement dit qui n'y occupent pas de

⁸⁹ Banques: art. 3 ss LB; bourses: art. 3 LBVM; négociants: art. 10 LBVM; directions de fonds de placement: art. 10 LFP.

⁹⁰ Pour une définition de la garantie d'une activité irréprochable dans ce contexte, voir Bulletin CFB 40/2000, p. 18, disponible sur l'internet: <http://www.ebk.admin.ch/f/publik/bulletin/bull40.pdf>.

⁹¹ Selon les nouvelles dispositions sur la responsabilité pénale de l'entreprise (art. 102 et 102a P-CP), cette dernière devrait à l'avenir également répondre pénalement de tels actes dans la mesure où elle n'aurait pas pris toutes les mesures raisonnables nécessaires pour empêcher la survenance de tels actes.

manière continue du personnel. Une exception est prévue pour les banques faisant partie d'un groupe financier soumis à une surveillance prudentielle. Mis à part cette exception, toutes relations d'affaires avec des «shell banks» sont interdites d'une manière générale (al. 2).

7.3 Mesures organisationnelles

Art. 7 Relations d'affaires comportant des risques accrus

Le degré de diligence applicable aux relations d'affaires doit être renforcé en fonction du risque potentiel accru que celles-ci présentent. Avant de pouvoir déterminer quelles relations comportent des risques accrus, l'intermédiaire financier devra définir les critères de risques qui correspondent à son domaine d'activité (al. 4). Les risques engendrés par une clientèle privée étrangère ne seront ainsi pas les mêmes que ceux auxquels s'expose une banque active exclusivement dans le domaine du retail en Suisse. Il suffira en principe de classer les relations en deux catégories selon qu'elles présentent ou non des risques accrus. En conséquence, certains clients seront considérés en tant que tels comme présentant un risque accru, sans que cela ne signifie qu'ils sont indésirables ou que l'établissement d'une relation avec eux est interdit. La conséquence en sera toutefois que des clarifications complémentaires devront être entreprises (art. 17). Cette classification doit en principe pouvoir se faire sur la base des informations immédiatement disponibles à l'ouverture d'un compte, sans engager de grandes recherches. Par ailleurs, les critères utilisés doivent être pertinents du point de vue des risques juridiques et des risques de réputation (al. 1). Ils peuvent se rapporter aussi bien au cocontractant qu'à l'ayant droit économique. En règle générale, cette répartition dans les différentes catégories de risques définies à l'intérieur d'un établissement devra avoir lieu lors de l'entrée en relation d'affaires⁹², étant entendu que certaines informations ne sont vérifiables qu'en cours de relation.

L'alinéa 2 procède à une énumération exemplative des critères qui

⁹² Cf. art. 20.

peuvent être utilisés. Cas échéant, plusieurs d'entre eux devront être utilisés conjointement pour entraîner la qualification d'une relation d'affaires comme relation à risque. Certains se réfèrent à des juridictions étrangères (lit. a, b et g). Aussi bien pour des raisons politiques que pratiques, la CFB n'établira pas de listes de pays à risques, mais communiquera certaines indications aux intermédiaires financiers en se fondant sur les travaux de forums internationaux tel que le GAFI, le cas échéant. Bien que la rencontre directe (lit. c) avec le client ne soit pas la panacée, elle contribue à une meilleure connaissance de la personnalité et de l'arrière-plan social et commercial du client. Par ailleurs, le comportement d'un client qui tenterait de se soustraire aux clarifications de l'intermédiaire financier serait suspect (indice A8 de l'annexe). Le type de prestations ou de produits sollicités (p.ex. comptes à numéros, opérations back to back, crédits fiduciaires) peut également, selon les circonstances et la spécialisation de l'intermédiaire financier, signifier un risque accru (lit. d). L'importance des valeurs patrimoniales remises peut également constituer un facteur de risque (lit. e). L'importance des entrées et sorties de valeurs patrimoniales (lit. f) doit être estimée sur la base de l'ensemble de l'activité du cocontractant et/ou de l'ayant droit économique.

En raison d'expériences du passé, les relations d'affaires nouées avec des PEP sont obligatoirement classées comme comportant des risques accrus (al. 3).

Art. 8 Transactions présentant des risques accrus

Le système exposé pour les relations d'affaires à risques s'applique *mutatis mutandis* aux transactions présentant des risques accrus. Comme exposé précédemment, les exigences possibles énumérées ne constituent pas des standards minimaux applicables à tous les intermédiaires financiers. Ils ne font qu'illustrer de possibles spécifications des systèmes de surveillance des transactions.

Toutefois, la fixation d'un montant limite (lit. a) au-delà duquel les transactions doivent être classées comme présentant des risques accrus devrait être possible pour toutes les banques. La vérification d'écarts significatifs par rapport au comportement habituel du client (lit. b) devrait être possible et, selon l'activité de l'intermédiaire financier, avoir un intérêt. Enfin, au vu de l'état actuel de la technique, il peut être raisonnable, en fonction de la composition de la clientèle et du volume de transactions d'un intermédiaire financier, d'installer un système de surveillance des transactions qui reconnaisse les divergences entre les transactions d'un client et celles du segment de clientèle auquel il appartient (lit. c). A cet effet, il est toutefois nécessaire que des groupes de clientèle puissent être définis de manière sensée, ce qui présuppose au moins un grand nombre de relations d'affaires comparables. Même dans ces conditions, un tel système ne se justifiera pas pour tous les intermédiaires financiers. Ceux-ci devront déterminer eux-mêmes, sur la base d'une analyse de leurs risques et de la structure de leurs relations d'affaires, quel type de surveillance des transactions est adéquat. Pour autant que l'analyse des risques à laquelle a procédé l'intermédiaire financier puisse être considérée comme raisonnable, la CFB ne substituera pas sa propre appréciation à celle de l'intermédiaire financier.

*Art. 9 Gestion globale des risques juridiques
et des risques de réputation*

Les intermédiaires financiers qui possèdent à l'étranger des succursales ou des sociétés de groupes doivent déterminer, limiter et contrôler de manière globale leurs risques de réputation. Les risques juridiques liés à la survenance d'un cas de blanchiment ou à la découverte d'actes terroristes d'une part ainsi que des articles de presse pouvant éventuellement porter atteinte à la renommée peuvent avoir des effets au-delà des frontières nationales sur l'ensemble des entités reliées entre elles. Par conséquent, il doit être possible de déterminer et contrôler d'une manière consolidée les relations avec des clients à

risques accrus de l'ensemble du groupe, même lorsque celles-ci sont nouées avec une succursale ou une filiale étrangère (al. 1).

A cet effet, les groupes financiers doivent notamment posséder un service Compliance au niveau du groupe qui doit avoir, en cas de nécessité, accès aux informations concernant les cocontractants et les ayants droit économiques de toutes les sociétés du groupe. En cas de nécessité, il doit être possible de faire vérifier la présence de certaines relations d'affaires dans l'ensemble des portfolios de toutes les unités juridiques ou d'affaires du groupe. Cette disposition est conforme à la pratique internationale des autorités de surveillance qui exige d'une manière générale la mise en place d'un système centralisé de gestion des risques couvrant l'ensemble du groupe sous la responsabilité d'un Group Compliance Officer⁹³. Pour la mise en œuvre de cette exigence, il existe au niveau international plusieurs pratiques. L'Ordonnance n'exige pas de banque de données centralisée, mais uniquement un accès aux données de clients des entités étrangères en cas de nécessité, ce qui correspond aux recommandations internationales⁹⁴. L'Ordonnance prévoit en outre que les sociétés du groupe à l'étranger doivent transmettre aux organes compétents de la centrale en Suisse les informations essentielles permettant de garantir une bonne gestion globalisée des risques juridiques et de réputation. Un tel cas se présentera par exemple lorsqu'il existe des indications selon lesquelles un client aurait des relations avec des organisations terroristes. Ces exi-

⁹³ Le Customer Due Diligence Paper du Comité de Bâle, cf. ch. 4.5 supra, requiert à son ch. 16 un contrôle consolidé des relations d'affaires importantes ("Customers frequently have multiple accounts with the same bank, but in offices located in different countries. To effectively manage the reputational, compliance and legal risk arising from such accounts, banks should be able to aggregate and monitor significant balances and activity in these accounts on a fully consolidated worldwide basis, regardless of whether the accounts are held on balance sheet, off balance sheet, as assets under management, or on a fiduciary basis."). Suite aux événements du 11 septembre 2001, cette exigence a été développée et la mise en place d'un système de gestion des risques centralisé aux fins d'une gestion globale des risques de réputation des groupes financiers est désormais considérée comme obligatoire. Cf. Basel Committee Publications No. 89, April 2002, Summary of a meeting of representatives of Supervisors and Legal Experts of G10 Central Banks and Supervisory Authorities on 14 December 2001, Basel, Switzerland, disponible sur l'internet sous <http://www.bis.org/publ/bcbs89.pdf>.

⁹⁴ Cf. également Sharing of financial records between jurisdictions in connection with the fight against terrorist financing, note 55 supra.

gences qui se réfèrent expressément aux sociétés de groupe sont (*ad maiore minus*) également applicables dans les rapports à l'intérieur d'une même entité juridique, soit par exemple entre les succursales et le siège d'une société (al. 2).

Dans l'hypothèse où l'accès direct des organes compétents du groupe à des informations concernant l'établissement étranger est empêché en raison de dispositions restrictives du droit étranger, la CFB doit en être informée. Elle devra rechercher, de cas en cas, une solution avec l'intermédiaire financier concerné et, le cas échéant, en contact avec les autorités de surveillance du pays d'accueil. En dernier recours, la CFB pourrait restreindre ou interdire l'établissement de succursales ou sociétés de groupes d'intermédiaires suisses dans la juridiction considérée (al. 3).

Les établissements suisses compris dans le périmètre de consolidation d'un intermédiaire financier étranger ou d'un groupe financier étranger doivent garantir l'accès des organes de contrôle de la société-mère étrangère aux informations portant sur ses clients et ayants droit économiques, dans la mesure où ces informations sont nécessaires à la surveillance consolidée des risques de réputation du groupe. La constitution d'une banque de donnée centralisée comprenant des informations sur la clientèle de l'établissement sis en Suisse n'est pas nécessaire dans ce cas non plus, ni d'ailleurs autorisée. Si cela devait se révéler nécessaire dans un cas d'espèce, un tel accès doit toutefois être possible pour les organes de la société-mère étrangère. Il ne peut en effet être refusé à ceux-ci ce que l'on exige des organes de contrôle d'intermédiaires financiers suisses par rapport à leurs établissements à l'étranger dans le cadre de la gestion globale des risques (al. 4).

Art. 10 Directives internes en matière de lutte contre le blanchiment

L'Ordonnance exige, comme les Directives sur le blanchiment de capitaux⁹⁵, des directives internes en matière de lutte contre le blanchi-

⁹⁵ Cf. ch. 15 Circ.-CFB 98/1.

ment. Elles devront être communiquées à toutes les collaboratrices et tous les collaborateurs concernés.

L'alinéa 2 règle le contenu minimal des directives. Les lettres a à d et i constituent des tâches nouvelles par rapport aux Directives sur le blanchiment de capitaux. Pour ce qui concerne les mesures que l'intermédiaire financier devra prendre pour déterminer, limiter et contrôler les risques accrus (lettre c), il y aura lieu entre autres de définir les procédures et les responsabilités applicables aux décisions à prendre suite à des clarifications complémentaires.

L'importance de la thématique justifie que ces directives fassent l'objet d'une décision formelle de la direction au moins et, par exemple pour les intermédiaires financiers ayant une petite structure, du conseil d'administration (al. 3).

Art. 11 Formation du personnel

Les collaboratrices et collaborateurs d'un intermédiaire financier doivent recevoir à leur entrée en fonction une formation en matière de blanchiment qui soit adaptée à leur position. Cette formation doit être mise à jour de manière régulière pour tous les collaborateurs et toutes les collaboratrices concernés par la lutte contre le blanchiment.

Art. 12 Systèmes de surveillance des transactions

L'art. 6 LBA exige des intermédiaires financiers qu'ils éclaircissent l'arrière-plan économique et le but des transactions inhabituelles, lorsque la légalité de celles-ci n'est pas manifeste. A cet effet, il y a lieu, dans une première phase, de détecter les transactions inhabituelles. Dans la mesure où ils ne le font pas déjà, les intermédiaires financiers devront mettre en place un système informatique les aidant à déceler les transactions présentant des risques accrus (al. 1). L'Ordonnance permet une définition flexible des paramètres du système en fonction du domaine d'activité de l'intermédiaire financier considéré⁹⁶. L'introduction

⁹⁶ Cf. supra, commentaire ad art. 8.

de tels logiciels nécessitant un grand investissement en temps, il en a été tenu compte dans la fixation des délais transitoires de l'Ordonnance⁹⁷.

Ces systèmes informatiques ne constituent qu'un moyen auxiliaire. En fin de compte, ce sont les collaboratrices et collaborateurs responsables de l'intermédiaire financier qui devront examiner la pertinence des rapports générés par le système. Les transactions qui ne pourront être expliquées immédiatement de manière plausible devront faire l'objet de clarifications complémentaires. Les données dégagées par le système ne doivent pas être examinées simultanément à l'exécution des opérations, mais dans un délai raisonnable. Il n'est pas exigé de l'intermédiaire financier qu'il s'assure de la légalité d'une transaction avant de l'exécuter. Finalement, il n'est pas non plus exigé que l'ensemble du trafic des paiements soit filtré afin de détecter d'éventuels donneurs d'ordre ou bénéficiaires «suspects» (al. 2).

Dans des petites structures, une surveillance des transactions informatisée peut se révéler trop coûteuse et donc disproportionnée, sans répondre à une nécessité absolue. Dans un tel cas de figure, l'intermédiaire financier pourra renoncer à mettre en place un système de surveillance informatisé, sans être toutefois dispensé de surveiller d'une autre manière les transactions. Il n'est pas possible de définir de manière abstraite une ligne de démarcation au-delà de laquelle les intermédiaires financiers pourront être dispensés de l'installation de tels systèmes informatisés. D'une manière générale, chaque intermédiaire financier est libre d'y renoncer dans la mesure où il est capable de surveiller les transactions «manuellement» d'une manière tout aussi efficace, ce qui ne devrait toutefois pas être simple. Dans ce cas, le réviseur externe devra en outre procéder annuellement à une révision approfondie se rapportant à l'existence et à l'efficacité de la surveillance systématique effectuée manuellement (al. 3).

⁹⁷ Cf. infra, commentaire ad art. 32.

Art. 13 Service interne de lutte contre le blanchiment

Dans la règle, le service interne de lutte contre le blanchiment sera vraisemblablement confié au département «Compliance» de l'intermédiaire financier, soit d'une manière générale, soit à une cellule de celui-ci. Le service interne de lutte contre le blanchiment n'est chargé que de tâches de conseil et d'assistance. La responsabilité relative aux relations d'affaires demeure auprès de la ligne. Cela signifie en particulier que les conseillères et les conseillers à la clientèle ne peuvent se dispenser de poser les questions nécessaires à leurs clients.

Le département «Compliance» prépare les directives internes en matière de lutte contre le blanchiment à l'attention de la direction⁹⁸ (al. 2 lit. a) et en contrôle l'exécution d'entente avec les réviseurs internes et externes ainsi que les responsables de la ligne (al. 2 lit. b). La responsabilité de l'organisation de la formation du personnel lui incombe (al. 2 lit. c)⁹⁹ de même que la fixation des paramètres de surveillance des transactions conformément à l'art. 12 (al. 2 lit. d). Le service interne de lutte contre le blanchiment ne procède en principe pas lui-même aux vérifications des avis générés par le système de surveillance des transactions, mais s'assure que les personnes de la ligne responsables à cet égard examinent régulièrement et avec diligence la pertinence de ces résultats (al. 2 lit. e). Dans les cas où des clarifications complémentaires doivent être entreprises, le service interne de lutte contre le blanchiment devra soit y procéder lui-même, soit en charger les personnes responsables de la ligne (al. 2 lit. f). Il doit s'assurer que l'organe compétent pour décider de l'admission ou de la poursuite d'une relation comportant un risque accru reçoit régulièrement la documentation nécessaire à sa prise de décision (al. 2 lit. g).

Les possibilités d'externalisation d'une telle structure sont formulées de manière relativement large, puisqu'elles sont ouvertes non seulement aux intermédiaires financiers qui ne sont pas en mesure de mettre sur pied un service en raison de leur taille ou de leur organisa-

⁹⁸ Art. 10 al. 3.

⁹⁹ Art. 11.

tion, mais également dans les cas où cela serait inapproprié eu égard aux circonstances, par exemple à cause de l'intégration de l'intermédiaire financier dans un groupe. Au surplus, les dispositions générales en matière d'externalisation¹⁰⁰ (outsourcing) sont applicables (al. 3).

7.4 Obligations de diligence générales

Art. 14 Vérification de l'identité du cocontractant et identification de l'ayant droit économique

D'une manière identique à ce que prévoit le ch. 10 des Directives sur le blanchiment de capitaux, l'applicabilité des dispositions de la CDB en matière de vérification d'identité du cocontractant et d'identification de l'ayant droit économique est étendue à tous les intermédiaires financiers soumis à la surveillance de la CFB en matière de blanchiment (al. 1). Contrairement au projet mis en consultation, l'Ordonnance ne mentionne pas la possibilité pour la CFB d'imposer des dispositions divergentes à celles de la CDB. Toutefois, cette compétence résulte pour la CFB de la loi sur le blanchiment¹⁰¹.

Art. 15 Indication des donneurs d'ordre lors de virements

Cette disposition met en œuvre la Recommandation VII des Recommandations spéciales du GAFI sur le financement du terrorisme¹⁰², aux termes de laquelle une information exacte et compréhensible doit être fournie sur le donneur d'ordre lors d'un virement. Les détails de la mise en œuvre de cette recommandation sont encore l'objet de discussions au niveau international. En février 2003, le GAFI adoptait le texte d'une note interprétative relative à la Recommandation VII¹⁰³. Cette note exige d'une manière générale la mention du nom et, dans la mesure où il existe un compte, du numéro de compte du donneur d'ordre. En outre, les ordres de transferts doivent indiquer l'adresse de

¹⁰⁰ Cf. Circ.-CFB 99/2 «Outsourcing».

¹⁰¹ Art. 16 et 41 LBA.

¹⁰² Cf. ch. 4.2 supra.

¹⁰³ Interpretative Note to FATF Special Recommendation VII: Wire Transfers, 13. Februar 2003: http://www.fatf-gafi.org/pdf/INSR7_en.PDF.

celui-ci, cette indication pouvant toutefois être remplacée soit par un numéro d'identité national, un numéro d'identification du client ou la date et le lieu de naissance du donneur d'ordre. Une exception est admise pour les virements nationaux dans la mesure où l'accès à ces informations est garanti aux autorités nationales compétentes.

La présente disposition s'inspire des exigences du GAFI. L'intermédiaire financier est ainsi tenu d'indiquer le nom, le numéro de compte et le domicile du donneur d'ordre de chaque transfert. L'indication du nom du donneur d'ordre est exigée dans tous les cas. Le reste des informations peut être remplacé par un numéro d'identification dans la mesure où celui-ci permet de reconnaître la transaction ou la relation d'affaires dans le cadre de laquelle la transaction est effectuée. En conformité avec les Recommandations du GAFI¹⁰⁴, ces exigences sont limitées au trafic de paiement international (alinéa 1).

Les intermédiaires financiers peuvent, lorsque le cocontractant justifie de motifs légitimes qu'ils éclaircissent et dont ils vérifient la plausibilité, renoncer à faire figurer certaines des informations relatives au donneur d'ordre selon l'alinéa 1. Les clarifications entreprises doivent être documentées (alinéa 2). L'indication du nom du cocontractant ne peut avoir lieu qu'avec l'accord de celui-ci. Cela signifie que la banque devra, avant l'exécution de virements vers l'étranger, rendre attentifs en particulier les titulaires de comptes à numéros au fait que leur nom devra dans la règle figurer dans la documentation accompagnant le transfert. Lors de virements effectués depuis des comptes nominatifs, le nom du cocontractant est en revanche déjà indiqué aujourd'hui de manière régulière, sauf instruction contraire du client.

Art. 16 Commerce professionnel de billets de banque

Aucune modification de la réglementation telle qu'elle est actuellement contenue dans la Directive sur le commerce professionnel de

¹⁰⁴ Cf. note 103.

billets de banque¹⁰⁵ n'est prévue. Le contenu de cette dernière a toutefois été notablement condensé.

7.5 Obligations de diligence accrues

Art. 17 Clarifications complémentaires en cas de risques accrus

L'art. 6 LBA prévoit une obligation particulière de clarifications en cas de transaction ou de relation d'affaires inhabituelles. L'Ordonnance répond à cette exigence et précise ce qui est attendu des intermédiaires financiers en la matière. Pour les clients ainsi que pour les transactions présentant des risques accrus, il est ainsi prescrit de procéder à des clarifications systématiques allant au-delà des mesures d'identification requises de manière routinière par la Convention de diligence lors d'une ouverture de compte. Le but de ces clarifications complémentaires est de se procurer des informations additionnelles au sujet du client et de son environnement qui permettent d'évaluer de manière plus précise le risque lié à la relation. Les données supplémentaires recueillies par le biais de ces clarifications constituent un profil-client. Il est toutefois renoncé à utiliser cette expression afin d'éviter des confusions avec des éclaircissements poursuivant un but différent, soit en particulier ceux tendant à une optimisation des prestations à la clientèle en matière de gestion de patrimoine et de négoce de valeurs patrimoniales. Naturellement, les informations récoltées pour ce dernier type de profil-client peuvent également servir dans le cadre de la lutte contre le blanchiment. En règle générale toutefois, les données obtenues dans un but de conseil ne satisferont pas aux exigences posées en matière de clarifications complémentaires. Par ailleurs, il faut relever que la réglementation en matière de protection des données¹⁰⁶ trouve pleine application dans la récolte et l'exploitation de ces informations.

Eu égard au grand nombre de relations d'affaires, il serait irréaliste d'exiger ce genre de clarifications pour tous les clients et n'apporterait

¹⁰⁵ Cf. supra ad art. 1^{er}.

¹⁰⁶ Loi fédérale sur la protection des données du 19 juin 1992, RS 235.1.

vraisemblablement pas de résultat satisfaisant. L'idée n'est pas d'entreprendre des clarifications de grande envergure d'une manière superficielle, mais au contraire de procéder à des éclaircissements approfondis ciblés en fonction des risques. L'investissement consenti par l'intermédiaire financier devra toutefois rester dans les limites du raisonnable (al. 1).

L'alinéa 2 énumère une liste non exhaustive de points qui, en fonction des circonstances, devront faire l'objet de clarifications en cas de relations ou transactions à risques accrus (p.ex. provenance des valeurs patrimoniales remises, origine de la fortune du client). Le but est de réunir autant d'informations que nécessaire à la constitution d'une solide base pour l'évaluation des risques. Dans cette recherche d'informations, l'intermédiaire financier est contraint de prendre l'initiative. Il doit faire suffisamment de recherches et ne peut se contenter d'explications peu probantes du client, même si les clarifications peuvent parfois se révéler délicates.

Les intermédiaires financiers sont autorisés à maintenir des relations d'affaires comportant des risques accrus dans la mesure où, sur la base des clarifications entreprises, ils parviennent à la conclusion que ces risques peuvent être supportés. Des relations d'affaires comportant des risques accrus ne représentent pas en tant que telles des relations indésirables ou interdites. Il en va de même pour les relations avec les PEP. L'intermédiaire financier doit toutefois connaître et évaluer les risques auxquels il s'expose.

Art. 18 Moyens de clarification

L'Ordonnance nomme quelques moyens à disposition pour effectuer les clarifications, à mettre en œuvre selon les circonstances. Elle se fonde principalement sur la constatation que la plausibilité des informations délivrées par le client doit généralement être vérifiée (al. 3). Les informations récoltées auprès du client (lit. a) sont toutefois aussi

bien utiles que nécessaires. Selon les circonstances, les informations obtenues par ce premier biais peuvent être complétées par des visites sur place (lit. b), par la consultation de sources publiquement accessibles telles que des banques de données disponibles sur l'internet (lit. c) voire par l'obtention de renseignements auprès de tiers dignes de confiance (lit. d). Ces derniers peuvent aussi bien être la banque précédente du client, un autre client de l'intermédiaire financier ou des bureaux spécialisés dans la recherche d'information de nature financière, cela à condition que le client y consente. A noter toutefois que toute publication négative au sujet d'un client ne doit pas nécessairement avoir pour conséquence de rendre celui-ci indésirable pour l'intermédiaire financier. A une époque où les médias pratiquent une information à sensation, parfois sans discernement ou de manière partisane, une grande prudence est de mise. L'intermédiaire financier doit cependant être en mesure de se faire une idée précise sur ses clients à risques accrus sur la base d'une information aussi complète que possible (al. 1).

Les clarifications complémentaires doivent avoir lieu dans le respect des droits de la personnalité du client et des autres personnes concernées. Cela signifie par exemple que la consultation de banques de données publiques devra être entourée de mesures assurant que des tiers ne puissent pas faire le lien entre l'intermédiaire financier et le client (al. 2).

Le résultat des clarifications doit être examiné de manière critique. Les conclusions que l'intermédiaire financier en a tirées doivent ensuite être documentées (al. 3).

Art. 19 Délégation des clarifications complémentaires à des tiers

En règle générale, l'intermédiaire financier procédera lui-même aux clarifications complémentaires. A certaines conditions, il lui est toutefois permis d'en charger des tiers. Il pourra s'agir par exemple de per-

sonnes mandatées au cas par cas tels des avocats. Il est aussi possible qu'un gérant de fortune externe entreprenne ces clarifications. Est également envisageable, une délégation à l'intérieur d'un groupe financier, p.ex. à une autre société du groupe ou au siège étranger d'une succursale en Suisse. Dans tous ces cas, l'Ordonnance en général et le présent article relatif à la délégation en particulier s'appliqueront. Cela sera le cas également dans l'hypothèse d'une délégation des clarifications complémentaires par la succursale suisse d'une banque étrangère au siège de ladite banque à l'étranger.

Dans la règle, les prescriptions en matière d'externalisation¹⁰⁷ ne trouveront pas application. Elles pourront toutefois s'appliquer dans la mesure où un intermédiaire financier établirait avec son délégataire un rapport durable de délégation des clarifications complémentaires. Cet article correspond à la disposition prévue dans la CDB pour la délégation dans le cadre de l'ouverture de comptes¹⁰⁸.

La délégation de clarifications complémentaires présuppose que l'intermédiaire financier conclue un contrat sous la forme écrite avec le délégataire, dans lequel il instruit précisément ce dernier de ses tâches. Elle devra se faire dans le respect des trois *curae*. L'intermédiaire financier devra s'assurer que le délégataire appliquera la même diligence que lui dans sa tâche (*cura in eligendo*, lit. a). En Suisse, tous les intermédiaires financiers soumis à la Loi sur le blanchiment répondent à ce critère. L'intermédiaire financier devra donner toutes les instructions nécessaires à la bonne exécution des clarifications (*cura in instruendo*, lit. b). Enfin, il devra avoir la possibilité de contrôler la qualité du travail du délégataire (*cura in custodiendo*, lit. c) (al. 1). La documentation relative aux clarifications doit être remise à l'intermédiaire financier. A l'avenir également, les clients conseillés par des gestionnaires de fortune externes et des fiduciaires devront être connus des banques et des négociants (al. 3).

¹⁰⁷ Circ.-CFB 99/2.

¹⁰⁸ Ch. 19^{quater} CDB 03.

En plus des trois *curae* précitées, l'intermédiaire financier devra encore examiner les informations qui lui sont transmises avec un œil critique. Il ne saurait en effet être question pour lui d'accepter toutes les informations qui lui sont rapportées sans se poser la question de leur plausibilité. En fin de compte, la responsabilité finale de la bonne exécution des clarifications lui incombera (al. 4).

Art. 20 Moment des clarifications complémentaires

Lorsque les risques accrus sont apparents au premier contact avec le client, l'intermédiaire financier doit procéder immédiatement aux clarifications complémentaires. Dans la règle, un compte ne devrait pas être rendu opérationnel avant l'accomplissement de cette procédure. Toutefois, les clarifications correspondantes peuvent nécessiter beaucoup de temps. Suivant les cas, une interdiction absolue d'utiliser un compte dans ce délai pourrait entraîner des situations délicates à gérer pour l'intermédiaire financier, sans forcément être justifiée par les circonstances. Cela d'autant moins que l'utilisation (temporaire) d'un compte, jusqu'à ce que le résultat des clarifications soit connu, serait mieux à même de faciliter une éventuelle enquête portant sur l'existence d'un blanchiment d'argent qu'un refus pur et simple des valeurs patrimoniales.

Contrairement à la solution retenue par la CDB¹⁰⁹, il a donc été renoncé à fixer un délai absolu à l'intérieur duquel le compte ne doit pas être activé. En fin de compte, il appartient à l'intermédiaire financier d'apprécier les risques potentiels qu'il encourt dans le cas d'espèce. Cela ne doit toutefois pas conduire à des reports sans fin sur des mois ou des années. L'exigence minimale est d'entreprendre les clarifications immédiatement et de les conduire sans retard, que le risque apparaisse en début ou en cours de relation. Dans l'hypothèse où aucune information pertinente ne peut être obtenue dans un délai raisonnable, la relation doit être communiquée ou interrompue¹¹⁰.

¹⁰⁹ Ch. 21^{bis} CDB.

¹¹⁰ Cf. art. 27 s.

Art. 21 Admission de relations d'affaires comportant des risques accrus

L'admission d'une nouvelle relation à risques accrus requiert l'approbation d'un supérieur hiérarchique ou d'une instance désignée à cet effet au sein de l'établissement. Pour ce qui est de la décision relative à l'entrée en relation d'affaires avec un PEP, celle-ci devra, comme c'est déjà le cas actuellement, être prise au niveau de la direction¹¹¹. Dans la mesure où, après réévaluation, une relation est classée comme comportant des risques accrus alors qu'elle n'avait pas été considérée comme telle lors de son admission, une approbation de l'instance ad hoc doit être recherchée pour la poursuite de la relation.

Art. 22 Responsabilité de la direction à son plus haut niveau

Les décisions relatives à des relations présentant des risques accrus sont par principe du ressort de la hiérarchie supérieure. Les conseillers et conseillers à la clientèle directement concernés ne doivent pas pouvoir décider, faute de posséder la distance nécessaire dans certains cas. La direction à son plus haut niveau ne doit pas non plus pouvoir se décharger de la responsabilité de ces décisions parfois désagréables sur des responsables de ligne subalternes ou sur le service interne de lutte contre le blanchiment. La tâche de ce dernier est toutefois de réunir l'ensemble de la documentation devant servir à la direction pour sa prise de décision¹¹². A l'opposé, doit également être évitée une règle de compétence qui contraindrait la direction à son plus haut niveau à prendre un grand nombre de décisions sur la base d'une profusion d'informations que, de manière réaliste, elle ne peut pas assimiler.

Dans la règle et conformément à ce qui est déjà prévu dans les Directives sur le blanchiment de capitaux, un membre au moins de la direction à son plus haut niveau sera ainsi responsable de la décision relative à l'admission ou au maintien d'une relation avec un PEP. Il est renoncé à une réglementation équivalente pour toutes les relations à risques accrus en raison de la probable impossibilité pour la direction

¹¹¹ Art. 22 al. 1 lit.a.

¹¹² Cf. art. 13 al. 2 lit. g.

de remplir correctement sa tâche dans tous les cas, le nombre de relations concernées pouvant en effet être très important dans certains établissements¹¹³. La direction sera toutefois responsable d'ordonner et de surveiller des contrôles réguliers de toutes les relations présentant des risques accrus et d'évaluer le résultat de ces contrôles (al. 1).

Ce règlement de compétence est inadapté aux grandes banques qui possèdent des structures de hiérarchie complexes. Une autre solution plus adéquate devra être trouvée au cas par cas, qui tiendra toutefois compte de l'idée de base de la présente disposition. (al. 2)

7.6 Devoirs de documentation

Art. 23 Disponibilité de l'information

Cette disposition précise l'art. 7 de la Loi sur le blanchiment, lequel prévoit une obligation d'établir et de conserver les documents relatifs aux transactions et aux clarifications. Il y a lieu de permettre aux autorités de poursuite pénale entre autres de se faire une idée sur les transactions et les relations d'affaires concernées ainsi que sur le respect de la Loi sur le blanchiment.

La lettre c reprend l'obligation pour les intermédiaires financiers d'être en mesure de donner suite à une demande d'information relative à des personnes détenant une procuration sur un compte¹¹⁴, ce qui nécessite généralement la tenue d'un registre des fondés de procuration. Cette exigence se rapporte aux procurations générales, à l'exception des procurations spéciales. Par ailleurs, les procurations publiées dans un registre officiel tel que le Registre du commerce ne doivent pas nécessairement y figurer. Doit également être documenté le résultat de clarifications complémentaires relatives à des relations d'affaires comportant des risques accrus (art. 18 al. 3) ou des transactions (art. 12 al. 2).

¹¹³ Cf. toutefois art. 21.

¹¹⁴ Cf. ch. 37 s. Circ.-CFB 98/1.

7.7 Comportement en présence d'indices de blanchiment ou de liens avec des organisations terroristes

Ce chapitre précise et complète les devoirs généraux des art. 9 à 11 LBA applicables à tous les intermédiaires financiers. La réglementation de la Loi sur le blanchiment, en particulier les dispositions relatives au devoir de communiquer en cas de soupçon fondé de blanchiment, sont pleinement applicables. Il n'est pas nécessaire d'en répéter les principes dans l'Ordonnance.

Art. 24 Communication lors de l'établissement d'une relation d'affaires

A l'image des Directives sur le blanchiment de capitaux¹¹⁵, cette disposition précise le comportement que doit adopter l'intermédiaire financier en cas de soupçon fondé de blanchiment ou de lien avec le terrorisme avant qu'une relation d'affaires n'ait été établie. En application des art. 4 s., l'intermédiaire financier sera amené à refuser d'ouvrir un compte dans de telles circonstances. Dans ce cas également, une communication au sens de l'art. 9 LBA doit être faite lorsque le soupçon fondé est manifeste.

Art. 25 Liens avec une organisation terroriste

Il s'agit d'une précision du devoir de communication dans le cas d'indices de liens avec des activités terroristes. La Loi sur le blanchiment en général et l'art. 9 en particulier restent fondamentalement applicables. Conformément à la Convention sur le financement du terrorisme¹¹⁶, ce devoir prend effet en présence de simples éléments permettant d'établir un lien direct ou indirect entre une transaction ou une relation d'affaires et une organisation terroriste. Ce sera par exemple le cas lorsque le nom d'une des personnes impliquées dans une relation d'affaires figure sur les listes de présumés terroristes émises par les autorités.

Art. 26 Comportement en l'absence de décision des autorités

Cet article reprend et précise l'art. 10 al. 2 de la Loi sur le blanchiment

¹¹⁵ Cf. ch. 22 Circ.-CFB 98/1.

¹¹⁶ Cf. art. 18 lit. b iii; cf. également ch. 4.6 supra.

dans le sens de la réglementation actuelle¹¹⁷. En l'absence de notification d'une décision des autorités pénales compétentes dans le délai légal, l'intermédiaire financier peut décider sur la base de sa propre appréciation si et dans quelle mesure il entend poursuivre la relation d'affaires¹¹⁸. Dans un tel cas de figure, les règles du droit civil entrent à nouveau en jeu et le cocontractant est naturellement habilité à retirer ses fonds ou clore la relation dans les limites du contrat qui le lie à l'intermédiaire financier. Afin d'exclure tout doute, il serait souhaitable que les autorités de poursuite pénale fassent connaître à l'intermédiaire financier les motifs qui les ont poussées à ne pas prononcer de blocage.

Art. 27 Doutes sur la qualité d'une relation d'affaires et droit de communication

Il arrive que, en raison des risques de réputation encourus, des intermédiaires financiers souhaitent rompre (en maintenant le «paper trail» conformément à l'art. 28) une relation d'affaires, alors même qu'ils ne possèdent pas de soupçon fondé que les valeurs patrimoniales concernées proviennent d'un crime. Dans un tel cas de figure, il est possible que les valeurs patrimoniales soient transférées auprès d'un autre intermédiaire financier pour lequel les doutes conçus par l'intermédiaire financier qui clôt la relation ne seront pas visibles de prime abord. En particulier lorsque sont en jeu d'importantes valeurs patrimoniales, cette manière de se débarrasser d'une relation encombrante est susceptible de porter sérieusement atteinte à la réputation de la place financière. Dans un tel cas, l'Ordonnance exige de l'intermédiaire financier qu'il examine l'exercice de son droit de communication sur la base de l'art. 305^{ter} al. 2 du Code pénal et qu'il documente le résultat de cet examen. Il n'existe toutefois pas de devoir de communication (al. 2).

Art. 28 Rupture de relations d'affaires douteuses

L'intermédiaire financier qui rompt une relation d'affaires sur la base

¹¹⁷ Cf. ch. 32 Circ.-CFB 98/1.

¹¹⁸ Cf. toutefois art. 29.

de simples doutes – et donc sans faire usage de son droit de communication – peut transférer les fonds sous une forme qui sauvegarde le «paper trail» (al. 1), à moins qu’une mesure de blocage des autorités ne soit imminente. Cette règle également correspond au droit en vigueur¹¹⁹.

Art. 29 Poursuite de relations d'affaires douteuses

L’intermédiaire financier possède naturellement le droit de poursuivre une relation d’affaires douteuse au sens de l’art. 27, qu’il ait renoncé à faire usage de son droit de communication ou que, après avoir communiqué la relation au Bureau de communication, aucune décision ne lui ait été notifiée par les autorités pénales compétentes¹²⁰. Toutefois, il y aura lieu de maintenir la relation sous un contrôle plus strict, sur la base notamment des constatations faites à l’occasion de l’examen de l’exercice du droit de communication. L’intermédiaire financier pourra prévoir une procédure interne de surveillance de ce type de relation.

Art. 30 Information de la Commission des banques

Cette disposition reprend la réglementation actuelle¹²¹. Aux termes de l’art. 23^{bis} al. 2 de la Loi sur les banques, la CFB est habilitée à exiger des banques et des réviseurs toutes les informations nécessaires pour l’exécution de ses tâches.

7.8 Révision

Art. 31 Contrôle par les réviseurs externes

Cette disposition formalise l’obligation des réviseurs externes de contrôler, dans le cadre de leurs révisions annuelles, l’observation par l’intermédiaire financier des exigences de l’Ordonnance. Les réviseurs doivent se prononcer sur ce point de manière expresse dans leurs rapports de révision ordinaires. D’éventuelles violations de l’Ordonnance

¹¹⁹ Cf. ch. 29 Circ.-CFB 98/1.

¹²⁰ Cf. art. 26. A fortiori lorsque le Bureau de communication informe l’intermédiaire financier qu’il n’est pas donné de suite à la communication.

¹²¹ Ch. 34 Circ.-CFB 98/1.

(ou de la CDB) doivent être mentionnées expressément. Dans le cas de groupes financiers, chaque société de groupe assujettie à la surveillance de la CFB aux termes de l'art. 2 al. 2 doit être mentionnée séparément. La CFB se réserve le droit, le cas échéant, d'ordonner en sus des contrôles approfondis, des révisions extraordinaires, voire d'entreprendre elle-même des contrôles sur place.

7.9 Dispositions finales

Art. 32 Dispositions transitoires

Les délais transitoires fixés tiennent compte du fait que l'Ordonnance a été soumise en consultation au cours de l'été 2002, qu'elle a été publiée par la Commission des banques et communiquée aux intéressés dans sa version définitive début 2003. Il ne peut toutefois pas être exclu que, dans certains cas particuliers, les travaux de mise en œuvre des nouvelles mesures – p.ex. pour ce qui a trait à la classification des relations existantes – pourraient se révéler notablement plus importants qu'escompté. Pour cette raison, la possibilité de présenter une requête de prolongation des délais à la CFB a été prévue (al. 1).

La détermination des relations d'affaires comportant des risques accrus doit avoir lieu pour l'ensemble des relations d'affaires, soit également pour celles qui sont déjà établies à l'entrée en vigueur de l'Ordonnance. L'intermédiaire financier n'est pas tenu de procéder à cet effet à un examen rétrospectif des transactions effectuées (al. 2). Dans la mesure où l'intermédiaire financier n'a pas encore procédé aux clarifications complémentaires, celles-ci doivent être exécutées aussi rapidement que possible.

Les systèmes de surveillance des transactions doivent être opérationnels dès le 1^{er} juillet 2004. Ils doivent permettre de filtrer, sur la base des paramètres définis, les transactions inhabituelles exécutées dès cette date (al. 3).

Afin de permettre une évaluation plus aisée des rapports attendus concernant la mise en œuvre de l'Ordonnance, les intermédiaires financiers recevront un questionnaire standardisé qu'ils devront remplir et adresser à leurs réviseurs externes pour approbation avant de le transmettre à la Commission des banques (al. 4).

Il incombe aux réviseurs des intermédiaires financiers de contrôler la mise en œuvre de l'Ordonnance¹²². Ce contrôle relève des tâches de la révision ordinaire. Les réviseurs doivent rendre compte de cette mise en œuvre par les intermédiaires financiers la première fois dans leurs rapports pour l'année 2004 et se prononcer sur le respect des exigences de l'Ordonnance dans ce cadre (al. 5).

Les intermédiaires financiers qui sont déjà soumis à la surveillance de la CFB en matière de blanchiment aux termes du ch. 5 des Directives sur le blanchiment de capitaux et qui désirent bénéficier du régime de l'art. 2 al. 2, devront déposer une requête correspondante auprès de la CFB d'ici à la fin septembre 2003. Les requêtes devront être motivées conformément aux exigences qui ressortent de l'art. 2 al. 2 (al. 6).

¹²² Cf. art. 31.

Principales modifications par rapport au projet soumis en consultation

Sont à relever les modifications suivantes par rapport au projet soumis en consultation:

- L'Ordonnance renonce à un élargissement de la définition des personnes politiquement exposées (PEP) aux PEP qui ne sont plus en fonction, afin d'éviter que d'anciens PEP ne doivent être classés comme clients à risque leur vie durant. Les parlementaires ont également été ôtés de la définition (art. 1 lit. a OBA-CFB).
- L'Ordonnance rend explicite le fait que l'énumération des critères devant servir à répertorier les relations d'affaires comportant des risques accrus n'est pas exhaustive et précise au surplus que seule une désignation à usage interne est exigée. «L'absence de rencontre avec le cocontractant ainsi qu'avec l'ayant droit économique» est mentionnée comme critère supplémentaire (art. 7 OBA-CFB).
- «Des divergences significatives par rapport aux types de transactions pratiquées habituellement dans le cadre de relations comparables, par rapport aux volumes et aux fréquences de ces transactions» constituent un critère supplémentaire devant signaler les transactions présentant des risques accrus (art. 8 OBA-CFB).
- Lors de la délégation de clarifications complémentaires à des tiers, l'intermédiaire financier est tenu de s'assurer que les personnes ou entreprises choisies appliquent la même diligence que lui-même. Il doit leur donner des instructions quant à leurs tâches et être en mesure de contrôler l'exécution diligente des clarifications. Une sous-délégation par le délégataire est interdite. L'intermédiaire financier est tenu d'examiner lui-même le résultat des clarifications du point de vue de leur plausibilité (art. 19 OBA-CFB).
- L'Ordonnance exige que l'intermédiaire financier examine l'exercice de son droit de communiquer en particulier dans le cas de relations

d'affaires comportant d'importantes valeurs patrimoniales et qu'il documente le résultat de cet examen (art. 27 OBA-CFB).

- La disposition relative à la poursuite d'une relation d'affaires sous surveillance spéciale qui était déjà contenue dans la Circulaire 98/1 est reprise dans l'Ordonnance (art. 29 OBA-CFB).
- L'intermédiaire financier est tenu d'informer la CFB des communications qu'il effectue auprès du Bureau de communication, lorsqu'elles concernent des relations d'affaires comportant d'importantes valeurs patrimoniales ou lorsqu'il est vraisemblable, au vu des circonstances, que l'affaire aura des conséquences sur la réputation de l'intermédiaire financier ou celle de la place financière (art. 30 OBA-CFB).
- L'Ordonnance statue expressément que son respect constitue un point de révision pour les réviseurs externes qui devront inclure dans leur rapport de révision une prise de position correspondante (art. 31 OBA-CFB).

Fassung vom 17. Januar 2003

**Vereinbarung
über die Standesregeln zur Sorgfaltspflicht der Banken
(VSB 03)**

zwischen

der Schweizerischen Bankiervereinigung («Bankiervereinigung»)

einerseits

und

den unterzeichneten Banken («Banken»)

anderseits

vom 2. Dezember 2002

Einleitung

Art. 1 Präambel

- Im Bestreben, das Ansehen des schweizerischen Bankgewerbes im In- und Ausland zu wahren,
- in der Absicht, die bei der Aufnahme von Geschäftsbeziehungen und im Zusammenhang mit dem Bankgeheimnis geltenden Regeln einer einwandfreien Geschäftsführung zu umschreiben,
- im Willen, einen wirkungsvollen Beitrag zur Bekämpfung der Geldwäscherei und der Terrorismusfinanzierung zu leisten,

verpflichten sich die Banken gegenüber der Bankiervereinigung als der mit der Wahrung der Interessen und des Ansehens des schweizerischen Bankgewerbes betrauten Dachorganisation in diesen Standesregeln

- a) ihre Vertragspartner zu identifizieren und in Zweifelsfällen eine Erklärung des Vertragspartners über den an den Vermögenswerten wirtschaftlich Berechtigten einzuholen;
- b) keine aktive Beihilfe zur Kapitalflucht zu leisten;
- c) keine aktive Beihilfe zur Steuerhinterziehung und dergleichen zu leisten durch Abgabe von unvollständigen oder irreführenden Bescheinigungen.

1 ¹ Den Standesregeln unterstehen die beigetretenen Banken mit sämtlichen in der Schweiz domizilierten Geschäftsstellen, nicht aber ihre ausländischen Niederlassungen, Vertretungen und Tochtergesellschaften (vgl. aber Ziff. 11, 19 und 21).

² Die Banken dürfen ihre ausländischen Zweigniederlassungen und ihre ausländischen, im Bank- oder Finanzbereich tätigen Konzerngesellschaften nicht dazu missbrauchen, diese Vereinbarung zu umgehen.

2 Die Standesregeln ändern an der Pflicht zur Wahrung des Bankgeheimnisses nichts. Sie können und wollen nicht

- die ausländische Devisen-, Fiskal- und Wirtschaftsgesetzgebung gleichsam zum Bestandteil des schweizerischen Rechts erheben und für die Schweizer Banken beachtlich erklären (soweit dies nicht durch die geltenden Staatsverträge und die schweizerische Gesetzgebung bereits erfolgt ist);
 - die gegenwärtige Gerichtspraxis auf dem Gebiete des internationalen Rechts unterlaufen;
 - bestehende zivilrechtliche Verhältnisse zwischen Bank und Kunden ändern.
- 3 In den Standesregeln sind geltende Regeln einer den guten Sitten entsprechenden Bankführung verbindlich festgelegt. Sie sollen bestimmte im Geldwäschereigesetz geregelte Sorgfaltspflichten (Art. 3 – 5 GwG) sowie den Begriff der «nach den Umständen gebotenen Sorgfalt» bei der Entgegennahme von Vermögenswerten (Art. 305^{ter} StGB) konkretisieren¹. Die besonderen Abklärungspflichten bei Geschäftsbeziehungen oder Transaktionen mit erhöhtem Risiko sind Gegenstand der GwV-EBK. – Das normale Bankgeschäft soll dadurch nicht erschwert werden.

¹ Über die sinngemässe Anwendung der VSB auf das Geschäft der Kreditkartenorganisationen bestehen separate Regeln.

A Identifikation des Vertragspartners und Feststellung der wirtschaftlich Berechtigten

Art. 2 Identifikation des Vertragspartners

¹ Die Banken sind verpflichtet, bei Aufnahme einer Geschäftsbeziehung den Vertragspartner zu identifizieren.

² Dies gilt für:

- die Eröffnung von Konten oder Heften;
- die Eröffnung von Depots;
- die Vornahme von Treuhandgeschäften;
- die Vermietung von Schrankfächern;
- die Annahme von Aufträgen zur Verwaltung von Vermögen, die bei Dritten liegen;
- die Ausführung von Handelsgeschäften über Effekten, Devisen sowie Edelmetalle und andere Waren (Commodities) über Beträge von mehr als Fr. 25 000.–;
- Kassageschäfte über Beträge von mehr als Fr. 25 000.–.

I. Geltungsbereich

- 4 Die Pflicht zur Prüfung der Identität gilt unter Vorbehalt von Ziff. 18 unabhängig davon, ob Konti, Hefte und Depots jeglicher Art oder Schrankfächer unter dem Namen des Vertragspartners oder unter einer Nummer geführt werden (Art. 9).
- 5 Bei Inhabersparheften ist zu identifizieren, wer Einlagen oder Rückzüge von mehr als Fr. 25 000.– tätigt. Auf die Eröffnung neuer Inhabersparhefte ist zu verzichten.
- 6 Unter Effekten sind vereinheitlichte und zum massenweisen Handel geeignete Wertpapiere, nicht verurkundete Rechte mit gleicher Funktion (Wertrechte) und Derivate zu verstehen (vgl. Art. 2 lit. a BEHG). Zudem fallen darunter auch nicht standardisierte Finanzprodukte.

- 7 Unter Kassageschäften sind Bargeschäfte am Schalter (Geldwechsel, Kauf und Verkauf von Edelmetall, Barzeichnung von Kassa- und Anleiheobligationen, Barverkauf von Travellerchecks, Bareinlösen von Checks usw.) zu verstehen. Bareinzahlungen und Barbezüge in Verbindung mit bestehenden Konten/Heften sowie Ein- und Auslieferungen verbriefter Effekten in Verbindung mit bestehenden Depots gelten nicht als Kassageschäfte (Ziff. 5 bleibt vorbehalten).
- 8 ¹ Bei Geschäften unterhalb der Mindestgrenzen (Art. 2, Abs. 2, 6. und 7. Lemma) ist der Vertragspartner zu identifizieren, wenn die Identifikation offensichtlich durch Aufspalten der Beträge auf mehrere Transaktionen umgangen wird (sog. Smurfing).
- ² Bestehen Verdachtsmomente, dass Vermögenswerte aus Quellen stammen, wie sie in Art. 9 Abs. 1 GwG aufgeführt sind, so ist der Vertragspartner unabhängig von Mindestgrenzen (Art. 2 Abs. 2, 6. und 7. Lemma) oder Ausnahmen von der formellen Identifikation (Ziff. 18) zu identifizieren. Dies gilt nicht, wenn die Bank ein Geschäft oder das Eingehen einer Geschäftsbeziehung ablehnt.

II. Identifikation des Vertragspartners

1. Natürliche Personen
 - a) bei persönlicher Vorsprache
- 9 Bei persönlicher Vorsprache prüft die Bank die Identität des Vertragspartners, indem sie einen amtlichen Ausweis mit Fotografie (Pass, Identitätskarte, Führerausweis o.ä.) einsieht und fotokopiert sowie die nach Ziff. 22 erforderlichen Angaben festhält.
- b) bei Aufnahme der Geschäftsbeziehung auf dem Korrespondenzweg

10 Wird die Geschäftsbeziehung auf dem Korrespondenzweg oder über Internet aufgenommen, so prüft die Bank die Identität des Vertragspartners, indem sie sich eine echtheitsbestätigte Kopie eines Identifikationsdokuments im Sinne von Ziff. 9 zustellen und zudem die Wohnsitzadresse des Vertragspartners durch Postzustellung oder auf andere, gleichwertige Weise bestätigen lässt.

11 ¹ Die Bestätigung über die Echtheit der Kopie des Identifikationsdokuments kann ausgestellt werden durch

- a) eine Niederlassung, Vertretung oder Konzerngesellschaft der Bank,
- b) eine Korrespondenzbank oder einen anderen Finanzintermediär, der von der eröffnenden Bank zu diesem Zweck speziell ausgewählt worden ist,
- c) einen Notar oder eine andere öffentliche Stelle, die solche Echtheitsbestätigungen üblicherweise ausstellt.

² Als gültige Identifikation gilt auch eine bei der Postzustellung oder -abholung anhand eines amtlichen Ausweises erfolgte Identifikation, sofern damit die Zustellung ausschliesslich an den Adressaten gewährleistet ist.

2. Juristische Personen und Gesellschaften

- a) mit Sitz in der Schweiz

12 Die Bank vergewissert sich, ob die Firma des Vertragspartners im Schweizerischen Handelsamtsblatt publiziert oder auf einer öffentlichen Internetseite für Handelsregistereinträge verzeichnet ist (z.B. www.zefix.ch). Die Bank darf auch einschlägige privat herausgegebene Verzeichnisse und Datenbanken verwenden (Schweizerisches Rationenbuch etc.). Andernfalls ist die Identität aufgrund eines Handelsregisterauszugs festzustellen.

13 Die Identität der im Handelsregister nicht eingetragenen juristi-

schen Personen und Gemeinschaften (Vereine, Stiftungen, Stockwerkeigentümergeinschaften, selbständige öffentlich-rechtliche Anstalten und Körperschaften) ist anhand von Statuten oder gleichwertigen Dokumenten zu prüfen.

b) mit Sitz im Ausland

- 14 Die Identitätsprüfung dieser Vertragspartner hat aufgrund eines Handelsregistrauszugs, aufgrund eines gleichwertigen Ausweises oder aufgrund von Auszügen aus öffentlichen Internetseiten für Handelsregistrauszüge resp. gleichwertigen Ausweisen zu geschehen, aus welchem das Bestehen der juristischen Person oder Gesellschaft abgeleitet werden kann (z.B. «certificate of incorporation»).

c) Gemeinsame Bestimmungen

- 15 Der Handelsregistrauszug oder der gleichwertige Ausweis darf nicht älter als 12 Monate sein. Ein älterer Ausweis kann zusammen mit einem bis zu 12 Monate alten Testat einer Revisionsstelle oder einem «certificate of good standing» verwendet werden.
- 16 Bei der Identifikation von im Handelsregister nicht eingetragenen Vereinen, Stiftungen und Gemeinschaften sind auch die Eröffner, soweit sie zeichnungsberechtigt sind, zu identifizieren und zu dokumentieren.
- 17 ¹ Ist die Identität einer juristischen Person als Vertragspartner allgemein bekannt, so kann auf das Verfahren gemäss Ziff. 12 – 14 verzichtet werden. Die Identität gilt insbesondere dann als allgemein bekannt, wenn sie eine Publikumsgesellschaft oder direkt oder indirekt mit einer solchen verbunden ist. Verzichtet die Bank

auf das Verfahren gemäss Ziff. 12 – 14, so hält sie den Grund dazu aktenkundig fest.

² Das vereinfachte Verfahren gemäss Abs. 1 ist bei Sitzgesellschaften unzulässig, ausser bei solchen, die direkt oder indirekt mit einer Publikumsgesellschaft verbunden sind.

3. Ausnahmen

- 18 Die Identität eines Vertragspartners braucht nicht formell geprüft zu werden bei Eröffnung
 - a) eines Kontos, Depots oder Heftes lautend auf den Namen eines Minderjährigen durch eine mündige dritte Person, sofern im Zeitpunkt der Eröffnung Vermögenswerte von höchstens Fr. 25 000.– eingebracht werden; dafür ist die eröffnende mündige Person zu identifizieren; Ziff. 22 ist sinngemäss anwendbar; eröffnet der Minderjährige selbst ein Konto, Depot oder Heft, ist dieser selbst zu identifizieren;
 - b) eines Mieterkautionskontos für ein in der Schweiz gelegenes Mietobjekt;
 - c) eines Kontos zwecks Liberierung des Kapitals bei Gründung oder Kapitalerhöhung einer Aktiengesellschaft oder Gesellschaft mit beschränkter Haftung.
- 19 Ist ein Vertragspartner konzernintern in gleichwertiger Weise bereits identifiziert worden, so ist ein erneutes Verfahren gemäss Ziff. 9 – 14 nicht nötig. In diesen Fällen müssen bei den betroffenen Konzerneinheiten Kopien der ursprünglichen Identifikationsakten vorliegen. Vorbehalten bleiben Fälle, wo die gesetzlichen Bestimmungen diesen Datentransfer nicht zulassen.
- 20 Kann ausnahmsweise die Identität eines Vertragspartners nicht auf die vorgeschriebene Weise vorgenommen werden, z.B. weil eine Person über keine Identifikationspapiere verfügt oder weil

über eine öffentlichrechtliche Korporation oder Anstalt keine entsprechenden Unterlagen bestehen, so kann die Bank die Identität auf andere zweckdienliche Weise überprüfen, indem sie andere beweiskräftige Dokumente einsieht oder von öffentlichen Stellen entsprechende Bestätigungen oder für eine juristische Person das letzte Testat einer anerkannten Revisionsstelle einholt. Bestätigungen und Kopien von Ersatzdokumenten sind zu den Akten zu nehmen; ausserdem ist die Ausnahmesituation in einer Aktennotiz zu begründen.

4. Allgemeine Identifikationsvorschriften und Überwachung

- 21 ¹ Die Bank darf die Identifikation mittels einer schriftlichen Vereinbarung an Personen oder Unternehmen delegieren, wenn
- a. sie diese über ihre Aufgaben instruiert hat, und
 - b. sie kontrollieren kann, ob die Identifikationen richtig durchgeführt werden.
- ² Der Beauftragte hat die Identifikationsakten an die Bank zu übermitteln und zu bestätigen, dass übermittelte Kopien mit den Originalen übereinstimmen.
- ³ Eine Weiterdelegation durch den Beauftragten ist ausgeschlossen.
- 22 Auf geeignete Weise festzuhalten sind Name, Vorname, Geburtsdatum, Nationalität und Wohnsitzadresse bzw. Firma und domiciladresse des Vertragspartners, ebenso die Mittel, anhand derer die Identität geprüft worden ist. Stammt ein Vertragspartner aus einem Land, wo Geburtsdaten oder Wohnsitzadressen nicht verwendet werden, entfallen diese Angaben. Die Fotokopie des amtlichen Ausweises und andere Identifikationsakten sind aufzubewahren.
- 23 Die Bank hat sicherzustellen, dass die interne Revision und die

bankengesetzliche Revisionsstelle die Vornahme der Identifikation kontrollieren können.

- 24 Grundsätzlich müssen alle für die Identifikation erforderlichen Dokumente vollständig und in gehöriger Form vorliegen, bevor ein Konto benützt werden darf. Ausnahmsweise darf ein Konto vorher benützt werden, wenn die Bank durch ein Kontrollsystem sicherstellt, dass die fehlenden Unterlagen innerhalb von 30 Tagen eingehen. Rückzüge auf Verlangen des Kunden sind dabei nicht zulässig. Nach 30 Tagen wird das Konto gesperrt, falls die Unterlagen bis dahin nicht vollständig sind. Ist die Dokumentation nach 90 Tagen noch immer nicht komplett, so hat die Bank die Geschäftsbeziehung aufzulösen (vgl. auch Art. 6, Abs. 4).

Art. 3 Feststellung des wirtschaftlich Berechtigten

¹ Die Bank muss mit der nach den Umständen gebotenen Sorgfalt den wirtschaftlich Berechtigten feststellen. Bestehen Zweifel, ob der Vertragspartner mit dem wirtschaftlich Berechtigten identisch ist, verlangen die Banken vom Vertragspartner mittels Formular A eine schriftliche Erklärung darüber, wer der wirtschaftlich Berechtigte sei.

² Dies gilt für:

- die Eröffnung von Konten oder Heften;
- die Eröffnung von Depots;
- die Vornahme von Treuhandgeschäften;
- die Annahme von Aufträgen zur Verwaltung von Vermögen, die bei Dritten liegen;
- die Ausführung von Handelsgeschäften über Effekten, Devisen sowie Edelmetalle und andere Waren (Commodities) über Beträge von mehr als Fr. 25 000.–.

³ Bei Kassageschäften im Sinne von Art. 2 über Beträge von mehr als Fr. 25 000.– ist immer eine Erklärung des Vertragspartners über den wirtschaftlich Berechtigten zu verlangen. Die Banken halten

die Erklärung des Vertragspartners in geeigneter Weise fest. Es steht ihnen frei, ob sie dafür das Formular A verwenden wollen oder nicht.

- 25 ¹ Die Bank darf von der Vermutung ausgehen, dass der Vertragspartner mit dem wirtschaftlich Berechtigten identisch ist. Die Vermutung wird jedoch zerstört, wenn ungewöhnliche Feststellungen gemacht werden.

² Zweifel sind bei folgenden ungewöhnlichen Feststellungen angebracht:

- bei Erteilung einer Vollmacht an eine Person, welche erkennbar nicht in einer genügend engen Beziehung zum Vertragspartner steht; Verwaltungsvollmachten an Finanzintermediäre sind davon nicht erfasst;
- sofern der Bank die finanziellen Verhältnisse der Person, die eine Eröffnung gemäss Art. 3 beantragt, bekannt sind, und die mitgebrachten oder in Aussicht gestellten Werte ausserhalb dieses finanziellen Rahmens liegen;
- oder wenn der Kontakt mit dem Kunden andere aussergewöhnliche Feststellungen ergibt.

- 26 Bei Aufnahme der Geschäftsbeziehung auf dem Korrespondenzweg mit einer natürlichen Person ist in jedem Fall die Erklärung auf Formular A zu verlangen. Ausgenommen sind die in Ziff. 18 genannten Fälle.

- 27 Erklärt der Vertragspartner, ein Dritter sei der wirtschaftlich Berechtigte, so hat er dessen Namen, Vornamen, Geburtsdatum, Nationalität, Wohnadresse und Domizilstaat bzw. Firma, Domiziladresse und Domizilstaat mittels Formular A festzuhalten. Art. 3 Abs. 3 bleibt vorbehalten. Stammt ein wirtschaftlich Berechtigter aus einem Land, wo Geburtsdaten oder Wohnadressen nicht verwendet werden, entfallen diese Angaben.

- 28 Das Formular A kann vom Vertragspartner oder von einem von diesem Bevollmächtigten (mit schriftlicher Einzel- oder Generalvollmacht) unterzeichnet werden. Im Falle von juristischen Personen ist das Formular A oder die Vollmacht durch die in der Gesellschaftsdokumentation genannten Zeichnungsberechtigten zu unterzeichnen.
- 29 Bleiben ernsthafte Zweifel an der Richtigkeit der schriftlichen Erklärung des Vertragspartners bestehen und können diese nicht durch weitere Abklärungen ausgeräumt werden, so lehnt die Bank die Aufnahme der Geschäftsbeziehung oder die Ausführung des Geschäftes ab.
- 30 Formular A findet sich im Anhang dieser Standesregeln. Das Formular kann in deutscher, französischer, italienischer, spanischer und englischer Fassung bei der Geschäftsstelle der Schweizerischen Bankiervereinigung bezogen werden.
- 31 Es steht den Banken frei, eigene, ihren besonderen Bedürfnissen entsprechende Formulare herstellen zu lassen. Diese müssen aber den vollen Text des Musterformulars enthalten.
- 32 Im Falle von Sammelkonti und Sammeldepots hat der Konto- bzw. Depotinhaber der Bank eine vollständige Liste der wirtschaftlich Berechtigten mit den Angaben gemäss Ziff. 27 abzugeben und bei jeder Mutation diese der Bank unverzüglich mitzuteilen.
- 33 Bei kollektiven Anlageformen und Beteiligungsgesellschaften mit mehr als 20 wirtschaftlich Berechtigten als Investoren sind nur von jenen wirtschaftlich Berechtigten, die allein oder in gemeinsamer Absprache an den eingebrachten Vermögenswerten zu mindestens 5% berechtigt sind, die Angaben gemäss Ziff. 27 festzuhalten. Bei bis zu 20 wirtschaftlich Berechtigten sind die Angaben gemäss

Ziff. 27 von allen festzuhalten. Kollektive Anlageformen, die an einer Börse kotiert sind, haben keine Erklärung über die wirtschaftliche Berechtigung abzugeben.

- 34 ¹ Banken mit Sitz in der Schweiz oder im Ausland haben grundsätzlich keine Erklärung über die wirtschaftliche Berechtigung abzugeben. Für ihre Definition gelten die jeweiligen Spezialgesetze des Domizillandes. Erklärungen über die wirtschaftliche Berechtigung sind jedoch zu verlangen, wenn eine Bank, die keiner angemessenen Aufsicht und Regelung in Bezug auf die Bekämpfung der Geldwäscherei untersteht, für ungenannte Kunden Unterkonten führen lässt.

² Andere Finanzintermediäre mit Sitz, bzw. Wohnsitz in der Schweiz haben keine Erklärung über die wirtschaftliche Berechtigung abzugeben. Dasselbe gilt für im Ausland domizilierte andere Finanzintermediäre, die einer angemessenen Aufsicht und einer angemessenen Regelung in Bezug auf die Bekämpfung der Geldwäscherei unterstehen.

³ Als in- und ausländische andere Finanzintermediäre gelten: Fondsleitungen, Lebensversicherungs-Gesellschaften, Effektenhändler und steuerbefreite Einrichtungen der beruflichen Vorsorge im Sinn von Art. 2 Abs. 2 GwG. Für die Definition der ausländischen Finanzintermediäre gelten die entsprechenden Spezialgesetze des Domizillandes.

⁴ Ergeben sich Hinweise für Missbräuche einer Bank oder eines anderen Finanzintermediärs oder liegen generelle Warnungen der Eidgenössischen Bankenkommission oder der Bankiervereinigung über einzelne Institute oder über Institute eines bestimmten Landes vor, so sind auch von diesen eine Erklärung über die wirtschaftliche Berechtigung einzuholen oder andere Massnahmen zu ergreifen.

- 35 ¹ Die Delegation der Feststellung des wirtschaftlich Berechtigten

an Dritte ist möglich. Sie kann unter analoger Anwendung der Vorschriften von Ziff. 21 vorgenommen werden.

² Ziff. 24 ist auf die Feststellung des wirtschaftlich Berechtigten sinngemäss anwendbar.

- 36 Die Bank hat sicherzustellen, dass die interne Revision und die bankengesetzliche Revisionsstelle die Feststellung des wirtschaftlich Berechtigten kontrollieren können.
- 37 Vorbehalten bleiben die besonderen Bestimmungen über die Sitzgesellschaften und die Träger von Berufsgeheimnissen (Art. 4 und 5, Ziff. 38 – 46).

Art. 4 Verfahren bei Sitzgesellschaften

¹ Als Sitzgesellschaften im Sinne dieser Vereinbarung gelten alle Gesellschaften, Anstalten, Stiftungen, Trusts/Treuunternehmungen usw., die im Domizilstaat nicht einen Betrieb des Handels, der Fabrikation oder eines anderen nach kaufmännischer Art geführten Gewerbes führen.

² Von in- und ausländischen Sitzgesellschaften sind zu verlangen:

- a) zur Identifikation ein Handelsregistrauszug oder ein gleichwertiger Ausweis (vgl. Ziff. 12-16);
- b) zur Feststellung des wirtschaftlich Berechtigten eine Erklärung vom Vertragspartner mittels Formular A darüber, wer an den Vermögenswerten wirtschaftlich berechtigt sei.

³ Kennt die Bank den wirtschaftlich Berechtigten und verfügt sie über die Angaben gemäss Ziff. 27, so kann sie diese unter Verzicht auf das Formular A in einer Aktennotiz festhalten.

I. Sitzgesellschaft

- 38 Ohne Rücksicht auf Zweck, Funktion, Rechtsform und Sitz gelten (in- oder ausländische) Unternehmen als Sitzgesellschaften, wenn

- a) keine eigenen Geschäftsräume bestehen (Sitz bei einem Anwalt, bei einer Treuhandgesellschaft, bei einer Bank usw.) oder
 - b) kein eigenes, ausschliesslich für sie tätiges Personal angestellt ist oder das angestellte eigene Personal sich nur mit administrativen Arbeiten befasst (Führung der Buchhaltung, der Korrespondenz nach Weisung der die Sitzgesellschaft beherrschenden Personen oder Gesellschaften).
- 39 Als Sitzgesellschaften gelten auch Familienstiftungen sowie andere juristische Personen und Gesellschaften, welche die Wahrung der Interessen ihrer Mitglieder in gemeinsamer Selbsthilfe bezwecken oder politische, religiöse, wissenschaftliche, künstlerische, gemeinnützige, gesellige oder ähnliche Zwecke verfolgen, sofern die Bank feststellt, dass nicht ausschliesslich die genannten statutarischen Zwecke verfolgt werden.

II. Wirtschaftliche Berechtigung an einer Sitzgesellschaft

- 40 Wirtschaftlich Berechtigter an einer Sitzgesellschaft kann eine natürliche Person sein oder eine juristische Person, welche ein Handels-, Fabrikations- oder ein anderes nach kaufmännischer Art geführtes Gewerbe betreibt. Eine Sitzgesellschaft kann selbst nicht wirtschaftlich Berechtigte sein.
- 41 Die wirtschaftlich Berechtigten sind im Sinne der Ziff. 27 und 28 festzustellen und festzuhalten. Ziff. 29 ist anwendbar.
- 42 Ist eine Sitzgesellschaft an einer Börse kotiert, so müssen die daran wirtschaftlich Berechtigten nicht festgestellt werden.
- 43 Bei Personenverbindungen oder Vermögenseinheiten, an denen keine wirtschaftliche Berechtigung bestimmter Personen besteht (z.B. bei Discretionary Trusts), ist anstelle der Feststellung des

wirtschaftlich Berechtigten vom Vertragspartner eine schriftliche Erklärung zu verlangen, welche diesen Sachverhalt bestätigt. Die Erklärung hat ferner Angaben zu enthalten über effektive (nicht treuhänderische) Gründer und, falls bestimmbar, Personen, die dem Vertragspartner oder seinen Organen gegenüber instruktionsberechtigt sind, sowie den Kreis von Personen, die als Begünstigte in Frage kommen können (kategorieweise, z.B. «Familienangehörige des Gründers»). Sind Kuratoren, Protektoren usw. vorhanden, sind sie in der Erklärung aufzuführen.

- 44 Bei widerrufbaren Konstruktionen (z.B. Revocable Trusts) ist der effektive Gründer als wirtschaftlich Berechtigter aufzuführen.

III. Änderung der Unterschriftsberechtigung

- 45 Ändert im Geschäftsverkehr mit der Bank die Unterschriftsberechtigung für die Sitzgesellschaft, so hat die Bank das Verfahren von Art. 4 Abs. 2 lit. b zu wiederholen, ausser es sei offensichtlich oder werde von den leitenden Organen der Sitzgesellschaft oder ihren Zeichnungsberechtigten schriftlich bestätigt, dass sich die wirtschaftliche Berechtigung nicht geändert habe. Gelingt es nicht, über die wirtschaftliche Berechtigung Klarheit zu schaffen, ist Art. 6 Abs. 3 anwendbar.

Art. 5 Berufsheimnisträger

Die Banken können auf die Feststellung des wirtschaftlich Berechtigten bei Konten oder Depots, die im Namen von in der Schweiz zugelassenen Rechtsanwälten oder Notaren für Rechnung deren Klienten geführt werden, verzichten, sofern diese gemäss einer schriftlichen Erklärung des Rechtsanwaltes oder Notars ausschliesslich einem der folgenden Zwecke dienen und entsprechend gekennzeichnet (Art des Mandates) sind:

- a) – Abwicklung und damit, soweit tunlich, verbundene kurzfristige Anlage von Gerichtskostenvorschüssen, Kautionen, öffentlich-rechtlichen Abgaben etc. sowie von Zahlungen an oder von Parteien, Dritte(n) oder Behörden (Kennzeichnung «Klientengelder-Abwicklungskonto/-depot»);
- b) – Hinterlegung und damit, soweit tunlich, verbundene Anlage von Vermögenswerten aus einer hängigen Erbteilung oder Willensvollstreckung (Kennzeichnung z.B. «Erbchaft» oder «Erbteilung»);
 - Hinterlegung/Anlage von Vermögenswerten aus einer hängigen Güterausscheidung im Rahmen einer Ehescheidung oder -trennung (Kennzeichnung z.B. «Güterausscheidung Ehescheidung»);
 - Sicherheitshinterlegung/Anlage von Vermögenswerten in zivilrechtlichen oder öffentlich-rechtlichen Angelegenheiten (Kennzeichnung z.B. «Escrow-Konto/Depot», «Sperrdepot Aktienkauf», «Sicherheitshinterlegung Unternehmerkaution», «Sicherheitshinterlegung Grundstückgewinnsteuer» etc.).
 - Hinterlegung und damit, soweit tunlich, verbundene Anlage von Vermögenswerten in zivilrechtlichen oder öffentlich-rechtlichen Angelegenheiten vor ordentlichen Gerichten oder Schiedsgerichten und in Verfahren des Zwangsvollstreckungsrechts (Kennzeichnung z.B. «Vorschüsse», «Sicherstellung Gerichtskautions», «Konkursmasse», «Schiedsgerichtsverfahren» etc.).

46 ¹ Für die Erklärung nach Art. 5 besteht ein Formular R, das in deutscher, französischer und italienischer Sprache bei der Geschäftsstelle der Schweizerischen Bankiervereinigung in Basel bezogen werden kann.

² Von den Banken nach ihren besonderen Bedürfnissen hergestell-

te Formulare müssen den vollen Text des Musterformulars enthalten (vgl. Anhang).

Art. 6 Änderungen oder Mängel im Zusammenhang mit der Identifikation des Vertragspartners oder der Feststellung des wirtschaftlich Berechtigten (Art. 2 – 5)

¹ Die Bank hat das Verfahren gemäss Art. 2, Ziff. 9 – 24, und Art. 3 und 4, Ziff. 25 – 45, zu wiederholen,

- wenn im Lauf der Geschäftsbeziehung Zweifel aufkommen,
 - ob die gemachten Angaben über die Identität des Vertragspartners zutreffen,
 - ob der Vertragspartner mit dem wirtschaftlich Berechtigten identisch ist, oder
 - ob die abgegebene Erklärung über die wirtschaftliche Berechtigung zutrifft,
- wenn Anzeichen für nachträglich eingetretene Änderungen bestehen.

² Stellt eine Bank fest, dass eine Erklärung im Sinne von Art. 5 dieser Vereinbarung zu Unrecht ausgestellt worden ist, so hat sie vom Vertragspartner mittels Formular A die Erklärung über den wirtschaftlich Berechtigten zu verlangen. Wird die Erklärung über den wirtschaftlich Berechtigten nicht beigebracht, so ist die Geschäftsbeziehung abubrechen.

³ Die Banken sind verpflichtet, die Beziehungen zum Vertragspartner abubrechen, wenn sich aus dem Geschäftsverkehr der Verdacht aufdrängt, dass die Bank bei der Identifikation des Vertragspartners getäuscht worden ist, dass ihr bewusst falsche Angaben über den wirtschaftlich Berechtigten gemacht worden sind oder wenn auch nach Durchführung des Verfahrens gemäss Abs. 1 Zweifel an den Angaben des Vertragspartners weiterbestehen.

⁴ Die Beziehungen zum Vertragspartner dürfen nicht mehr abgebrochen werden, wenn die Voraussetzungen der Meldepflicht (Art. 9 GwG) gegeben sind.

- 47 Die laufenden Beziehungen sind so rasch abubrechen, als es ohne Vertragsverletzung möglich ist. Ist die Bank aufgrund von Korrespondenzinstruktionen nicht in der Lage, den Vertragspartner zu erreichen, so kann sie mit dem Abbruch der Beziehungen bis zu seinem nächsten Besuch bzw. bis zur nächsten Zustellung von Korrespondenz zuwarten.

B Verbot der aktiven Beihilfe zur Kapitalflucht

Art. 7 Kapitalflucht

Die Banken dürfen keine aktive Beihilfe zum Kapitaltransfer aus Ländern leisten, deren Gesetzgebung die Anlage von Geldern im Ausland einschränkt.

48 ¹ Kapitalflucht ist ein nicht autorisierter Kapitaltransfer in Form von Devisen, Noten oder Wertschriften aus einem Land, das diesen Transfer durch Deviseninländer ins Ausland verbietet oder beschränkt.

² Bloss Meldepflichten im Zusammenhang mit der Devisenausfuhr gelten nicht als Beschränkung des Kapitalverkehrs.

49 Auf den Kapitaltransfer aus der Schweiz ins Ausland ist Art. 7 nicht anwendbar.

50 Als Formen der aktiven Beihilfe gelten

- a) der organisierte Empfang von Kunden im Ausland ausserhalb der Räumlichkeiten der Bank zwecks Entgegennahme von Geldern;
- b) die Mitwirkung im Ausland bei der Organisation von Kompensationsgeschäften, wenn die Bank weiss oder nach den gesamten Umständen wissen muss, dass die Kompensation der Kapitalflucht dient;
- c) die aktive Zusammenarbeit mit Personen und Gesellschaften, welche die Kapitalflucht für Dritte organisieren oder dazu Hilfsdienste leisten, durch
 - Auftragserteilung;
 - Versprechen von Provisionen;
 - Führung ihrer Konten, wenn der Bank bekannt ist, dass diese Personen und Gesellschaften ihre Konten gewerbsmässig für Zwecke der Kapitalfluchthilfe benützen;

- d) das Hinweisen des Kunden auf unter lit. c genannte Personen und Gesellschaften.
- 51 Besuche bei Kunden im Ausland sind zulässig, sofern der Beauftragte der Bank dabei weder Geld entgegennimmt, dessen Transfer verboten ist, noch Ratschläge für den illegalen Kapitaltransfer erteilt, noch an Kompensationsgeschäften mitwirkt.
- 52 Im Übrigen dürfen Vermögenswerte ausländischer Kunden in der Schweiz entgegengenommen werden.

C Verbot der aktiven Beihilfe zu Steuerhinterziehung und ähnlichen Handlungen

Art. 8 Steuerhinterziehung und ähnliche Handlungen

Die Banken leisten Täuschungsmanövern ihrer Kunden gegenüber Behörden des In- und Auslandes, insbesondere gegenüber Steuerbehörden, weder durch unvollständige noch auf andere Weise irreführende Bescheinigungen Vorschub.

- 53 ¹ Verboten ist die Abgabe unvollständiger oder in anderer Weise irreführender Bescheinigungen an den Kunden selbst oder auf dessen Wunsch direkt an Behörden des In- oder Auslands.

² Unter Behörden sind namentlich Steuerbehörden, Zollämter, Währungs- und Bankenaufsichtsbehörden sowie Strafverfolgungsbehörden zu verstehen.

- 54 ¹ Unter das Verbot fallen besondere, vom Kunden zuhanden von Behörden angeforderte Bescheinigungen.

² Routinemässig erstellte Belege, wie Konto- und Depotauszüge, Gutschrifts- und Belastungsanzeigen, Abrechnungen über Devisengeschäfte, Coupons- und Börsenabrechnungen, dürfen von der Bank nicht zu Täuschungszwecken abgeändert werden.

- 55 ¹ Bescheinigungen sind unvollständig, wenn zur Täuschung von Behörden relevante Sachverhalte unterdrückt werden, indem z.B. die Bank auf Wunsch des Kunden in einer besonderen Bestätigung oder in einem Konto- oder Depotauszug einzelne Positionen weglässt.

² In Konto- und Depotauszügen braucht nicht erwähnt zu werden, dass für den gleichen Kunden noch andere Konten oder Depots geführt werden.

- 56 Bescheinigungen sind irreführend, wenn Sachverhalte zur Täu-

schung von Behörden wahrheitswidrig dargestellt werden, z.B. durch

- a) falsche Datierungen, falsche Beträge, fiktive Kurse oder die Angabe falscher Gutschriftsempfänger bzw. Belasteter;
- b) Bescheinigung fiktiver Forderungen oder Schulden (gleichgültig, ob die Bescheinigung den Büchern der Bank entspricht oder nicht);
- c) Zurverfügungstellen von bankeigenen Konti, sofern dies dem Kunden eine Verkürzung geschuldeter Fiskalabgaben ermöglicht.

D Übrige Bestimmungen

Art. 9 Nummernkonten

Auf unter Nummern oder Kennworten geführte Konten, Hefte, Depots und Schrankfächer sind die Vorschriften der vorliegenden Vereinbarung uneingeschränkt anwendbar.

- 57 In Bestätigungen über die gesamten Geschäftsbeziehungen zu einem Kunden sind auch die unter Nummern oder Kennworten geführten Konten und Depots, einschliesslich der Treuhandanlagen, einzubeziehen.

Art. 10 Kontrolle durch die Revisionsstellen

¹ Durch die Unterzeichnung dieser Standesregeln beauftragen und ermächtigen die Banken ihre bankengesetzliche Revisionsstelle, die Einhaltung der Standesregeln anlässlich der ordentlichen Bankenrevision stichprobenweise zu überprüfen und Verstösse oder den begründeten Verdacht von Verstössen der nach Art. 12 eingesetzten Aufsichtskommission sowie der Eidgenössischen Bankenkommision zu melden.

² Die Schweizerische Bankiervereinigung wird den anerkannten Revisionsstellen den Text dieser Standesregeln sowie die Liste der Unterzeichner und damit deren Auftrag bekanntgeben.

Art. 11 Verletzung der Standesregeln, Sanktionen

¹ Im Falle der Verletzung der Standesregeln hat die fehlbare Bank an die Bankiervereinigung eine Konventionalstrafe von bis zu Fr. 10 Mio. zu leisten. Bei der Bemessung der Konventionalstrafe sind die Schwere der Verletzung, der Grad des Verschuldens und die Vermögenslage der Bank gebührend zu berücksichtigen. Ausserdem ist von anderen Instanzen in der gleichen Sache verhängten Massnahmen Rechnung zu tragen. Die Höhe der Konventionalstrafe wird im Verfahren gemäss Art. 12 und allenfalls gemäss

Art. 13 bestimmt. Die Bankiervereinigung wendet die Konventionalstrafen nach Deckung des allfälligen Defizits der Kostenrechnung einem von ihr zu bestimmenden gemeinnützigen Zwecke zu.

² In Bagatelldfällen kann gegen die fehlbare Bank anstelle der Konventionalstrafe ein Verweis ausgesprochen werden.

³ Bei Verstößen gegen Art. 6 Abs. 1 und 2 wird eine Konventionalstrafe bzw. ein Verweis nur ausgesprochen, wenn sie grobfahrlässig, bei Verstößen gegen Art. 7 und 8, wenn sie vorsätzlich erfolgt sind.

⁴ Die Verletzung der Standesregeln wird nicht mehr verfolgt, wenn sie mehr als 5 Jahre zurückliegt. Bei Verstößen gegen die Pflicht zur Identifikation des Vertragspartners und zur Feststellung des wirtschaftlich Berechtigten beginnt die 5-Jahres-Frist mit der Behebung des Verstosses bzw. der Beendigung der Geschäftsbeziehung zu laufen.

Art. 12 Aufsichtskommission, Untersuchungsbeauftragte

¹ Für die Abklärung und Ahndung von Verletzungen dieser Standesregeln setzt die Bankiervereinigung eine aus fünf unabhängigen Persönlichkeiten bestehende Aufsichtskommission ein. Die Aufsichtskommission wählt einen Sekretär und regelt dessen Aufgaben.

² Die Bankiervereinigung bestimmt einen oder mehrere Untersuchungsbeauftragte. Sie stellen der Aufsichtskommission Antrag, entweder das Verfahren zu eröffnen und die angemessene Sanktion festzustellen oder die Ermittlungen einzustellen. In ihren Auskunftsbegehren geben sie der Bank bekannt, in welcher Eigenschaft sie in die Ermittlungen einbezogen wird.

³ Die Amtsdauer der Mitglieder der Aufsichtskommission und der Untersuchungsbeauftragten beträgt fünf Jahre. Wiederwahl ist zulässig.

⁴ Ergibt sich eine Verletzung der Standesregeln, stellt die Auf-

sichtskommission in Anwendung von Art. 11 hievor im Verfahren gegen die fehlbare Bank die angemessene Sanktion fest.

⁵ Die Aufsichtskommission ordnet das Verfahren und bestimmt über die Kostentragung.

⁶ Unterzieht sich die fehlbare Bank dem Beschluss der Aufsichtskommission, ist das Verfahren damit erledigt. Andernfalls gilt Art. 13 hienach.

⁷ Verweigert eine Bank die Mitwirkung bei den Untersuchungshandlungen der Aufsichtskommission oder eines Untersuchungsbeauftragten, so kann die Aufsichtskommission eine Konventionalstrafe im Sinne von Art. 11 aussprechen.

⁸ Als Beauftragte im Sinne von Art. 47 Bankengesetz haben die Mitglieder der Aufsichtskommission, der Sekretär und die Untersuchungsbeauftragten über die ihnen im Verfahren bekanntgewordenen Tatsachen strenge Verschwiegenheit zu wahren. Die Banken können gegenüber der Aufsichtskommission oder einem Untersuchungsbeauftragten das Bankgeheimnis nicht anrufen.

⁹ Die Aufsichtskommission gibt von ihren Entscheiden der Eidgenössischen Bankenkommision Kenntnis. Werden Missbräuche von Berufsgeheimnisträgern festgestellt, so kann die Aufsichtskommission ausserdem der entsprechenden Disziplinarinstanz Mitteilung machen.

- 58 Die Aufsichtskommission orientiert die Banken und die Öffentlichkeit periodisch und unter Wahrung des Bank- und Geschäftsgeheimnisses über ihre Entscheidungspraxis.
- 59 Die Aufsichtskommission kann – im Einvernehmen mit dem Verwaltungsrat der Bankiervereinigung – zuhanden der Banken Interpretationen zu den Standesregeln herausgeben. Banken richten entsprechende Gesuche an die Bankiervereinigung.

Art. 13 Schiedsverfahren

¹ Wird die von der Aufsichtskommission als angemessen festgesetzte Konventionalstrafe nach Fristansetzung nicht geleistet, hat auf Klage der Bankiervereinigung gegen die betreffende Bank ein Schiedsgericht mit Sitz in Basel über das Vorliegen einer Sorgfaltpflichtverletzung und die allenfalls deshalb auszufällende Vertragsstrafe endgültig zu entscheiden. Die Banken wählen zu diesem Zwecke Gerichtsstand in Basel.

² Die Bankiervereinigung und die Bank ernennen je einen Schiedsrichter und die beiden Schiedsrichter ernennen zusammen den Obmann des Schiedsgerichts.

³ Das Schiedsverfahren wird eingeleitet mit der Bezeichnung des von ihr zu bestimmenden Schiedsrichters durch die Bankiervereinigung.

⁴ Falls eine Partei ihren Schiedsrichter nicht innert 30 Tagen seit Erhalt der schriftlichen Mitteilung der anderen Partei betreffend die Einleitung des Schiedsverfahrens bezeichnet hat oder falls die beiden Schiedsrichter sich nicht innert 30 Tagen seit Annahme des Schiedsrichtermandats über die Ernennung des Obmanns einigen können, wird das Appellationsgericht des Kantons Basel-Stadt die Ernennung auf Verlangen einer Partei vornehmen.

⁵ Falls ein Schiedsrichter seine Funktion aus irgendwelchen Gründen nicht ausüben kann, muss die Partei, welche ihn ernannt hat, innert 30 Tagen einen neuen Schiedsrichter ernennen, ansonsten wird das Appellationsgericht des Kantons Basel-Stadt auf Verlangen der anderen Partei die Ernennung vornehmen.

⁶ Falls der Obmann seine Funktion aus irgendwelchen Gründen nicht ausüben kann, müssen die Schiedsrichter innert 30 Tagen einen neuen Obmann ernennen, ansonsten wird das Appellationsgericht des Kantons Basel-Stadt auf Verlangen einer Partei die Ernennung vornehmen.

⁷ Bei Ersetzung eines Schiedsrichters gemäss Abs. 5 und 6 hievorgelten die Prozesshandlungen, bei denen der ersetzte Schiedsrichter mitgewirkt hat, weiter.

⁸ Unter Vorbehalt gegenteiliger zwingender Vorschriften des Konkordats über die Schiedsgerichtsbarkeit und der ZPO BS gelten deren Bestimmungen nur, soweit die Parteien oder, falls diese auf ihr diesbezügliches Recht verzichten, das Schiedsgericht keine anderslautenden Verfahrensregelungen treffen. Die Eventualmaxime gilt frühestens im zweiten Schriftenwechsel.

⁹ Das Schiedsgericht untersteht der Verschwiegenheitspflicht von Art. 12 Abs. 8 ebenfalls.

Art. 14 Inkrafttreten

¹ Diese Standesregeln treten am 1. Juli 2003 in Kraft.

² Die Bankiervereinigung und jede unterzeichnende Bank können, unter Einhaltung einer Kündigungsfrist von drei Monaten auf das Ende eines Vertragsjahres, erstmals auf den 30. Juni 2008, von der Vereinbarung über die Standesregeln zurücktreten.

³ Die Bankiervereinigung behält sich vor – nach Rücksprache mit oder auf Begehren der Eidgenössischen Bankenkommission – den Banken während der Laufzeit der Vereinbarung ergänzende Regelungen bekanntzugeben (vgl. Art. 16 GwG).

⁴ Die Bankiervereinigung behält sich vor, das Sanktionssystem (Art. 11 – 13) einseitig anzupassen oder ausser Kraft zu setzen, sofern neue gesetzliche Vorschriften oder Rechtsentwicklungen zu einer stossenden mehrfachen Sanktionierung gleicher Sachverhalte führen sollten.

Art. 15 Übergangsbestimmung

¹ Die neuen Formulare A sind zu verwenden, wenn nach dem Datum des Inkrafttretens dieser Standesregeln eine Geschäftsbeziehung neu aufgenommen wird oder das Verfahren zur Feststellung des wirtschaftlich Berechtigten im Sinne von Art. 6 zu wiederholen ist.

² Die neuen Regeln über die Identifikation des Vertragspartners und die Feststellung des wirtschaftlich Berechtigten sind anzu-

wenden, wenn eine Geschäftsbeziehung nach dem Datum des Inkrafttretens dieser Standesregeln neu aufgenommen wird oder wenn das Verfahren zur Feststellung des wirtschaftlich Berechtigten im Sinne von Art. 6 nach Inkrafttreten dieser Standesregeln zu wiederholen ist. Auf bestehende Geschäftsbeziehungen finden die neuen Regeln Anwendung, sofern sie günstiger sind.

A

Kto-/Depot-Nr.:

Vertragspartner:

Feststellung des wirtschaftlich Berechtigten

(Formular A gemäss Art. 3 und 4 VSB)

Der Vertragspartner erklärt hiermit:

(Zutreffendes ankreuzen)

- ☐ dass der Vertragspartner allein an den Vermögenswerten wirtschaftlich berechtigt ist
- ☐ dass an den Vermögenswerten folgende Person/en wirtschaftlich berechtigt ist/sind:

Name, Vorname (evtl. Firma), Geburtsdatum, Nationalität, Wohnadresse/Sitz, Staat

Der Vertragspartner verpflichtet sich, der Bank Änderungen von sich aus mitzuteilen.

Das vorsätzlich falsche Ausfüllen dieses Formulars ist strafbar (Art. 251 des Schweizerischen Strafgesetzbuches, Urkundenfälschung; Strafandrohung: Zuchthaus bis zu fünf Jahren oder Gefängnis).

Ort, Datum

Unterschrift des Vertragspartners

R

Kto-/Depot-Nr.:

Vertragspartner:

Kennzeichnung:

Erklärung bei der Eröffnung eines Kontos oder Depots durch einen schweizerischen Anwalt oder Notar

Der/die Unterzeichnete erklärt hiermit, dass er/sie als Rechtsanwalt/Notar* tätig ist und der entsprechenden kantonalen Gesetzgebung untersteht.

Er/sie erklärt, dass er/sie an den jeweils eingebuchten Werten nicht selber wirtschaftlich berechtigt ist. Er/sie bestätigt, dass er/sie bezüglich des vorerwähnten Kontos/Depots **dem gesetzlichen Berufsgeheimnis (Art. 321 StGB) unterstellt ist und dass dieses Konto/Depot ausschliesslich dient:**

☐ der Abwicklung und der damit, soweit tunlich, verbundenen kurzfristigen Anlage von Gerichtskostenvorschüssen, Kautionen, öffentlich-rechtlichen Abgaben etc. sowie von Zahlungen an oder von Parteien, Dritte(n) oder Behörden (Kennzeichnung „Klientengelder-Abwicklungskonto/-depot“);

☐ der Hinterlegung und der damit, soweit tunlich, verbundenen Anlage von Vermögenswerten aus einer hängigen Erteilung oder Willensvollstreckung (Kennzeichnung z.B. „Erbchaft“ oder „Erteilung“);

der Hinterlegung und der damit, soweit tunlich, verbundenen Anlage von Vermögenswerten aus einer hängigen Güterausscheidung im Rahmen einer Ehescheidung oder -trennung (Kennzeichnung z.B. „Güterausscheidung Ehescheidung“);

der Sicherheitshinterlegung und der damit, soweit tunlich, verbundenen Anlage von Vermögenswerten in zivilrechtlichen oder öffentlich-rechtlichen Angelegenheiten (Kennzeichnung z.B. „Escrow-Konto/Depot“, „Sperrdepot Aktienkauf“, „Sicherheitshinterlegung Unternehmerkaution“, „Sicherheitshinterlegung Grundstückgewinnsteuer“ etc.);

der Hinterlegung und der damit, soweit tunlich, verbundenen Anlage von Vermögenswerten in zivilrechtlichen oder öffentlich-rechtlichen Angelegenheiten vor ordentlichen Gerichten oder Schiedsgerichten und in Verfahren des Zwangsvollstreckungsrechts (Kennzeichnung z.B. „Vorschüsse“, „Sicherstellung Gerichtskaution“, „Konkursmasse“, „Schiedsgerichtsverfahren“ etc.).

(Das zutreffende Feld ist anzukreuzen; es darf nur **ein Feld** angekreuzt werden).

Ort, Datum

Unterschrift

*Unzutreffendes bitte streichen

Das vorsätzlich falsche Ausfüllen dieses Formulars ist strafbar (Art. 251 des Schweizerischen Strafgesetzbuches, Urkundenfälschung; Strafandrohung: Zuchthaus bis zu fünf Jahren oder Gefängnis).

Version du 17 janvier 2003

**Convention
relative à l'obligation de diligence des banques
(CDB 03)**

entre

l'Association suisse des banquiers

d'une part

et

les banques signataires (ci-après «les banques»)

d'autre part

du 2 décembre 2002

Introduction

Art. 1 Preamble

- En vue de préserver le renom du système bancaire suisse sur les plans national et international,
- en vue d'établir des règles assurant, lors de l'établissement de relations d'affaires et dans le domaine du secret bancaire, une gestion irréfutable,
- en vue de contribuer efficacement à la lutte contre le blanchiment d'argent et le financement du terrorisme,

les banques s'obligent par la présente convention envers l'Association suisse des banquiers, en sa qualité d'organisation faîtière chargée de la sauvegarde des intérêts et de la réputation de la banque en Suisse, à:

- a) vérifier l'identité de leurs cocontractants et à se faire remettre, en cas de doute, une déclaration du cocontractant relative à l'ayant droit économique des valeurs patrimoniales confiées à la banque;
- b) ne prêter aucune assistance active à la fuite de capitaux;
- c) ne prêter aucune assistance active à la soustraction fiscale ou à des actes analogues, en délivrant des attestations incomplètes ou trompeuses.

- 1 ¹ Sont soumises à la convention les banques adhérentes et tous leurs comptoirs situés en Suisse, mais non pas leurs succursales, représentations et filiales à l'étranger (cf. toutefois ch. 11, 19 et 21).

² Les banques ne doivent pas utiliser leurs succursales étrangères et les sociétés du groupe à l'étranger actives dans le domaine bancaire ou financier, pour contourner la présente convention.

- 2 La convention ne modifie en rien l'obligation d'observer le secret bancaire. Elle ne peut et ne veut pas
 - étendre au territoire suisse le champ d'application de la législation étrangère en matière économique, fiscale et de change, et

- déclarer qu'elle doit être observée par les banques suisses (dans la mesure où les traités internationaux en vigueur et la législation suisse ne le prévoient pas déjà);
- s'écarter de la jurisprudence actuelle dans le domaine du droit international;
 - modifier les dispositions de droit civil qui régissent les rapports entre la banque et ses clients.
- 3 La convention assure la codification, avec effet contraignant, de règles en vigueur d'une gestion bancaire conforme à l'éthique professionnelle. Elle vise à concrétiser certaines obligations particulières de diligence prévues par la Loi sur le blanchiment d'argent (art. 3–5 LBA) ainsi que la notion de «vigilance que requièrent les circonstances» en matière d'acceptation de valeurs patrimoniales (art. 305^{ter} CPS)¹. Les devoirs de clarification complémentaire dans le cas de relations d'affaires ou de transactions présentant des risques accrus sont du ressort de l'OBA-CFB. – La convention ne doit pas constituer une entrave aux opérations bancaires normales.

¹ Des dispositions particulières déterminent l'application par analogie de la CDB aux organisations de cartes de crédit.

A Vérification de l'identité du cocontractant et identification de l'ayant droit économique

Art. 2 Vérification de l'identité du cocontractant

¹ Les banques s'engagent à vérifier l'identité du cocontractant dès qu'elles établissent des relations d'affaires avec lui.

² Cette règle s'applique à:

- l'ouverture de comptes ou de livrets;
- l'ouverture de dépôts;
- la conclusion d'opérations fiduciaires;
- la location de compartiments de coffre-fort;
- l'acceptation de mandats de gestion de fortune sur des avoirs déposés auprès de tiers;
- l'exécution d'opérations de négoce sur des valeurs mobilières, des devises ainsi que sur des métaux précieux et d'autres marchandises (Commodities) lorsqu'elles portent sur un montant supérieur à fr. 25 000.–;
- aux opérations de caisse, lorsqu'elles portent sur un montant supérieur à fr. 25 000.–.

I. Champ d'application

- 4 La vérification de l'identité est obligatoire, sous réserve du ch. 18, que les comptes, livrets et dépôts de tous genres ainsi que les compartiments de coffre-fort soient gérés sous le nom du cocontractant ou sous un numéro (art. 9 CDB).
- 5 Dans le cas de livrets d'épargne au porteur, l'identité de la personne qui effectue des dépôts ou des retraits supérieurs à fr. 25 000.– doit être vérifiée. Il n'est pas procédé à l'ouverture de nouveaux livrets d'épargne au porteur.
- 6 Par valeurs mobilières, on entend les papiers-valeurs standardisés,

susceptibles d'être diffusés en grand nombre sur le marché, les droits ayant la même fonction (droits-valeurs) et les dérivés (cf. art. 2 lit. a LBVM). Les produits financiers non standardisés en font également partie.

- 7 Les opérations de caisse comprennent les opérations au comptant effectuées au guichet d'une banque (change, achat et vente de métaux précieux, souscription au comptant à des bons de caisse et à des emprunts obligataires, vente au comptant de chèques de voyage, encaissement de chèques, etc.). Les versements et retraits au comptant sur des comptes/livrets déjà ouverts ainsi que les livraisons et retraits de valeurs mobilières sous forme de papiers-valeurs sur des dépôts déjà constitués ne sont pas considérés comme des opérations de caisse (le ch. 5 CDB demeure réservé).

- 8 ¹ Lors d'opérations portant sur un montant inférieur aux seuils susmentionnés (art. 2, al. 2, 6^{ème} et 7^{ème} tirets CDB), l'identité du cocontractant doit être vérifiée également, s'il apparaît que la vérification est contournée par la répartition des montants sur plusieurs transactions («Smurfing»).

² S'il existe des indices que des valeurs patrimoniales proviennent de l'une ou l'autre des sources énoncées à l'art. 9, al. 1 LBA, il faut vérifier l'identité du cocontractant, indépendamment de la limite chiffrée (art. 2, al. 2, 6^{ème} et 7^{ème} tirets CDB) ou des exceptions à l'obligation de vérifier formellement l'identité du cocontractant (ch. 18 CDB). Cette obligation ne s'applique pas lorsque la banque refuse une opération ou l'établissement de relations d'affaires.

II. Vérification de l'identité du cocontractant

1. Personnes physiques
 - a) Lors de pourparlers engagés par l'intéressé en personne avec la banque
- 9 Lorsque des pourparlers sont engagés par l'intéressé en personne avec la banque, cette dernière vérifie l'identité du cocontractant en examinant et en photocopiant une pièce de légitimation officielle comportant une photographie (passeport, carte d'identité, permis de conduire ou document analogue) ainsi qu'en relevant les indications prescrites au ch. 22 CDB.
 - b) Lorsque les relations d'affaires sont nouées par correspondance
- 10 Lorsque les relations d'affaires sont nouées par correspondance ou par internet, la banque vérifie l'identité du cocontractant en se faisant remettre une copie certifiée conforme d'un document d'identification au sens du ch. 9 et en obtenant, par un échange de correspondance ou par tout autre moyen adéquat, confirmation du domicile du cocontractant.
- 11 ¹ L'attestation d'authenticité de la copie du document d'identification peut être émise par
 - a) une succursale, une représentation ou une société appartenant au même groupe que la banque;
 - b) une banque correspondante ou un autre intermédiaire financier désigné spécialement à cet effet par l'établissement nouant la relation d'affaires;
 - c) un notaire ou une autre instance publique qui délivre habituellement de telles confirmations d'authenticité.² La vérification de l'identité peut également valablement être effectuée par le biais de la présentation d'une pièce de légitimation

officielle lors d'envois par la poste, s'il est ainsi garanti que l'envoi parvient au destinataire et à lui seul.

2. Personnes morales et sociétés

a) Avec siège en Suisse

- 12 La banque s'assure que la raison sociale du cocontractant a fait l'objet d'une publication dans la Feuille officielle suisse du commerce ou est publiée sur un site internet officiel procurant des extraits du Registre du commerce (par ex. www.zefix.ch). La banque peut également se référer aux banques de données et répertoires reconnus, publiés par des entreprises privées (Annuaire suisse du Registre du commerce etc.). Sinon, l'identité doit être établie par un extrait du Registre du commerce.

- 13 L'identité des personnes morales non inscrites au Registre du commerce et des indivisions (associations, fondations, communautés de copropriétaires par étage, établissements indépendants de droit public et corporations) est vérifiée sur la base des statuts ou de tout autre document équivalent.

b) Avec siège à l'étranger

- 14 L'identité de ces cocontractants est vérifiée sur la base d'un extrait du Registre du commerce, d'une pièce équivalente, ou encore sur la base de données prélevées sur un site internet officiel publiant des extraits du Registre du commerce ou des pièces équivalentes. Le document de référence doit permettre de déduire l'existence de la personne morale ou de la société (par exemple «certificate of incorporation»).

c) Dispositions communes

- 15 L'extrait du Registre du commerce ou la pièce équivalente ne doit pas dater de plus de 12 mois. Une pièce de légitimation plus ancienne peut être admise, mais seulement si elle est accompagnée du rapport du dernier exercice signé par l'organe de révision ou d'un «certificate of good standing», lesquels ne doivent pas dater de plus de 12 mois.
- 16 Lors de la vérification d'identité de sociétés, fondations et indivisions qui ne sont pas inscrites au Registre du commerce, la banque doit aussi vérifier l'identité et garder photocopie de la pièce de légitimation des personnes qui ont établi la relation d'affaires, dans la mesure où ces dernières sont signataires autorisées.
- 17 ¹ Lorsque l'identité d'une personne morale intervenant comme co-contractant est notoirement connue, il peut être renoncé à la procédure prévue par les ch. 12 à 14 CDB. L'identité est notoirement connue lorsque les actions de la société en question sont largement réparties dans le public ou lorsqu'elle est liée directement ou indirectement à une telle société. Si la banque renonce à la procédure prévue par les ch. 12 à 14 CDB, elle en indique le motif au dossier.
- ² La procédure simplifiée au sens du premier alinéa n'est pas admise pour les sociétés de domicile, à l'exception de celles qui sont liées directement ou indirectement à une société dont les actions sont largement réparties dans le public.

3. Exceptions

- 18 Il n'est pas nécessaire de vérifier formellement l'identité du co-contractant en cas d'ouverture:

- a) d'un compte, un dépôt ou un livret au nom d'un mineur par une tierce personne majeure, si les valeurs patrimoniales déposées lors de l'ouverture n'excèdent pas fr. 25 000.-. Il convient en revanche de vérifier l'identité de la personne majeure qui ouvre le compte, dépôt ou livret; le ch. 20 est applicable par analogie. Si le mineur ouvre lui-même le compte, dépôt ou livret, il convient de vérifier son identité;
 - b) d'un compte destiné au dépôt de sûretés pour garantir le paiement d'un loyer, pour autant toutefois que l'objet loué soit situé en Suisse;
 - c) d'un compte destiné à la libération du capital-actions, lors de la fondation ou d'une augmentation de capital d'une société anonyme ou d'une société à responsabilité limitée.
- 19 Lorsque l'identité du cocontractant a déjà été vérifiée au sein du groupe de façon équivalente, il n'est pas nécessaire de répéter la procédure prévue par les ch. 9 à 14 CDB. En ce cas, des copies des documents ayant servi à la vérification initiale de l'identité doivent être conservées dans les dossiers des entités concernées du groupe. Demeurent réservés les cas dans lesquels des dispositions légales interdisent ce transfert de données.
- 20 A titre exceptionnel, la banque peut vérifier l'identité du cocontractant d'une autre manière que celle prescrite ci-dessus, par ex. lorsqu'une personne ne dispose pas de pièce de légitimation ou lorsque, pour une corporation ou un établissement de droit public, les documents requis habituellement n'existent pas. Dans de tels cas la banque peut vérifier l'identité d'une autre manière appropriée, en examinant d'autres documents probants ou en se procurant auprès d'instances publiques des attestations à cet effet, ou encore pour les personnes morales, en obtenant le rapport du dernier exercice signé par l'organe de révision. Les attestations et copies des documents de substitution doivent être versées au dos-

sier. Par ailleurs, il convient de faire une note pour le dossier, énonçant les raisons pour lesquelles le cas est exceptionnel.

4. Prescriptions générales en matière de vérification de l'identité et surveillance

21 ¹ La banque peut, sur la base d'une convention écrite, déléguer la vérification de l'identité à des personnes ou entreprises, si:

- a. la banque les a instruits au sujet de leurs devoirs, et
- b. la banque est en mesure de contrôler si les vérifications de l'identité ont été correctement exécutées.

² Les personnes ou entreprises chargées de la vérification de l'identité doivent remettre les documents d'identification à la banque et doivent confirmer que les copies remises sont conformes aux originaux.

³ Les personnes ou entreprises chargées de la vérification de l'identité ne sont pas autorisées à sous-déléguer leur mandat.

22 Il y a lieu de conserver de manière appropriée le nom, le prénom, la date de naissance, la nationalité et l'adresse du domicile (la raison sociale et le siège, s'il s'agit d'une personne morale ou d'une société) du cocontractant, ainsi que les moyens utilisés pour vérifier son identité. Lorsque le cocontractant provient d'un pays dans lequel les dates de naissance ou les adresses de domicile ne sont pas utilisées, l'exigence relative à ces données ne s'applique pas. La photocopie de la pièce de légitimation officielle et les autres documents ayant servi à vérifier l'identité doivent être conservés.

23 La banque prend des dispositions garantissant que l'organe de révision interne et l'institution de révision prévue par la Loi sur les banques puissent contrôler que les vérifications prescrites ont été effectuées.

- 24 En règle générale, tous les documents exigés pour la vérification de l'identité doivent avoir été obtenus dans la forme appropriée, avant que le compte concerné puisse être opéré. A titre exceptionnel, un compte peut être opéré sans attendre que tous les documents précités soient au dossier, à condition que la banque soit en mesure d'assurer par un système de contrôle adéquat, que les pièces manquantes lui parviendront dans un délai de 30 jours. Dans l'intervalle, des retraits à la demande du client ne sont pas autorisés. A l'échéance du délai de 30 jours, le compte sera bloqué si les documents au dossier restent incomplets. Si, la documentation reste incomplète au-delà de 90 jours, la banque doit mettre fin à la relation d'affaires (cf. aussi Art. 6, al. 4).

Art. 3 Identification de l'ayant droit économique

¹ La banque doit identifier l'ayant droit économique avec le soin approprié aux circonstances. Lorsqu'il y a doute sur le point de savoir si le cocontractant est lui-même l'ayant droit économique, la banque exige une déclaration écrite au moyen d'un formulaire A indiquant qui est l'ayant droit économique.

² Cette règle s'applique à:

- l'ouverture de comptes ou de livrets;
- l'ouverture de dépôts;
- la conclusion d'opérations fiduciaires;
- l'acceptation de mandats de gestion de fortune sur des avoirs déposés auprès de tiers;
- l'exécution d'opérations de négoce sur des valeurs mobilières, des devises ainsi que sur des métaux précieux et d'autres marchandises (Commodities) lorsqu'elles portent sur un montant supérieur à fr. 25 000.-;

³ Lors d'opérations de caisse au sens de l'art. 2 CDB portant sur un montant supérieur à fr. 25 000.-, une déclaration du cocontractant relative à l'ayant droit économique doit toujours être exigée. Les banques conservent la déclaration du cocontractant de manière

appropriée. Elles sont libres d'utiliser ou non le formulaire A à cette fin.

- 25 ¹ La banque peut présumer que le cocontractant est aussi l'ayant droit économique. Mais cette présomption est détruite si des constatations insolites sont faites.

² Il y a doute dans les cas suivants:

- lors de la remise d'une procuration à une personne qui ne saurait manifestement avoir des liens suffisamment étroits avec le cocontractant. Les procurations de gestion octroyées à des intermédiaires financiers ne sont pas visées;
- lorsque la situation financière de la personne qui veut effectuer l'une des opérations décrites à l'art. 3 CDB est connue de la banque et que les valeurs remises ou sur le point de l'être sont hors de proportion avec la situation financière de cette personne;
- ou lorsque, dans le cadre de ses relations avec le client, la banque est amenée à faire d'autres constatations insolites.

- 26 Lors de l'établissement de relations d'affaires par correspondance avec une personne physique, la déclaration sur formulaire A doit être exigée dans tous les cas. Font exception les cas mentionnés au ch. 18 CDB.

- 27 Si le cocontractant déclare que l'ayant droit économique est un tiers, il doit indiquer au moyen d'un formulaire A le nom, le prénom, la date de naissance, la nationalité, l'adresse de domicile et le pays du domicile de ce tiers (la raison sociale, le siège et l'Etat du siège, s'il s'agit d'une personne morale ou d'une société). L'art. 3, al. 3 CDB demeure réservé. Lorsque l'ayant droit économique provient d'un pays dans lequel les dates de naissance ou les adresses de domicile ne sont pas utilisées, l'exigence de ces données ne s'applique pas.

- 28 Le formulaire A peut être signé par le cocontractant ou par un fondé de procuration (légitimé par une procuration écrite spécifique ou générale). Dans le cas des personnes morales, le formulaire A ou la procuration doit être signé par les personnes autorisées à signer en vertu de la documentation de la société.
- 29 Si des doutes sérieux persistent quant à l'exactitude de la déclaration écrite du cocontractant et si ceux-ci ne peuvent être levés par d'autres éclaircissements, la banque refuse d'entrer en relation d'affaires ou s'abstient d'exécuter l'opération en question.
- 30 Le formulaire A est annexé à la présente convention. Ce formulaire peut être obtenu en version française, allemande, italienne, espagnole et anglaise auprès du secrétariat de l'Association suisse des banquiers.
- 31 Les banques ont le droit de faire imprimer leurs propres formulaires, correspondant à leurs besoins particuliers. Ces formulaires doivent contenir le texte intégral du formulaire modèle.
- 32 En ce qui concerne les comptes globaux et les dépôts globaux, le titulaire du compte ou du dépôt doit fournir à la banque une liste exhaustive des ayants droit économiques comportant les indications prévues au ch. 24 CDB et communiquer immédiatement à la banque toute modification.
- 33 Dans les formes de placement collectif et sociétés de participations qui regroupent plus de 20 ayants droit économiques en qualité d'investisseurs, les indications prescrites au ch. 27 CDB ne sont exigées que pour les ayants droit économiques qui, seuls ou de concert, détiennent au moins 5% des valeurs patrimoniales déposées. Lorsque le nombre des ayants droit économiques est inférieur ou égal à 20, les indications prescrites au ch. 27 CDB doivent

être retenues pour chacun d'entre eux. Il n'y a pas lieu d'exiger une déclaration relative à l'ayant droit économique pour les formes de placement collectif qui sont cotées en bourse.

- 34 ¹ Aucune déclaration relative à l'ayant droit économique n'est en principe exigée des banques dont le siège est en Suisse ou à l'étranger. Par banques, on entend les établissements définis comme tels par les lois correspondantes de l'Etat de leur siège. Il convient toutefois d'exiger des déclarations relatives à l'ayant droit économique lorsqu'une banque qui n'est pas assujettie à une surveillance et à une réglementation appropriées en matière de lutte contre le blanchiment d'argent, fait ouvrir des sous-comptes pour des clients non spécifiés.

² Aucune déclaration relative à l'ayant droit économique n'est exigée des autres intermédiaires financiers dont le domicile ou le siège est en Suisse. La même règle vaut pour les autres intermédiaires financiers dont le domicile ou le siège se situe à l'étranger et qui sont assujettis à une surveillance appropriée ainsi qu'à une réglementation appropriée en matière de lutte contre le blanchiment d'argent.

³ Sont réputés autres intermédiaires financiers suisses et étrangers: les directions de fonds de placement, les compagnies d'assurance sur la vie, les négociants en valeurs mobilières et les institutions de prévoyance professionnelle exemptées d'impôts tels que définis par l'art. 2 al. 2 LBA. Pour la définition des intermédiaires financiers étrangers, les lois correspondantes de l'Etat de leur siège sont applicables.

⁴ Toutefois, la déclaration relative à l'ayant droit économique sera exigée ou d'autres mesures seront prises lorsque des indications révèlent qu'une banque ou un autre intermédiaire financier commet des abus ou lorsque la Commission fédérale des banques ou l'Association suisse des banquiers ont émis des mises en garde de

portée générale sur certains établissements en particulier ou sur les établissements d'un pays déterminé.

- 35 ¹ La délégation de l'identification de l'ayant droit économique est autorisée aux mêmes conditions que celles mentionnées au ch. 21.
² Le ch. 24 est applicable par analogie à l'identification de l'ayant droit économique.
- 36 La banque prend des dispositions garantissant que l'organe de révision interne et l'institution de révision prévue par la Loi sur les banques puissent contrôler l'identification de l'ayant droit économique.
- 37 Demeurent réservées les dispositions particulières relatives aux sociétés de domicile et aux personnes tenues au secret professionnel (art. 4 et 5, ch. 38–46 CDB).

Art. 4 Procédure relative aux sociétés de domicile

¹ Sont réputés sociétés de domicile au sens de la présente convention toutes les sociétés, établissements, fondations, trusts/entreprises fiduciaires, etc., qui n'exercent pas dans l'Etat de leur siège une activité de commerce ou de fabrication, ou une autre activité exploitée en la forme commerciale.

² Les banques doivent exiger des sociétés de domicile suisses et étrangères:

- a) un extrait du Registre du commerce ou une pièce équivalente (cf. ch. 12–16), en vue de la vérification de leur identité;
- b) une déclaration, établie sur formulaire A, par laquelle le co-contractant indique qui est l'ayant droit économique des valeurs patrimoniales.

³ Lorsque la banque connaît l'ayant droit économique et dispose des indications prescrites par le ch. 27 CDB, elle peut renoncer à l'utilisation du formulaire A en enregistrant ces informations au dossier.

I. Sociétés de domicile

- 38 Sont réputées sociétés de domicile, sans égard à leur but, à leur fonction, à leur forme juridique et à leur siège, les entreprises (suissees ou étrangères) qui
- a) ne disposent pas de leurs propres locaux (siège auprès d'un avocat, d'une société fiduciaire, d'une banque, etc.) ou
 - b) n'ont pas de personnel propre, travaillant exclusivement pour elles, ou dont le personnel propre n'est occupé qu'à des tâches administratives (tenue de la comptabilité et de la correspondance sur instructions des personnes ou sociétés dominant la société de domicile).
- 39 Sont également réputées sociétés de domicile, les fondations de famille ainsi que d'autres personnes morales et sociétés qui ont pour but la sauvegarde des intérêts de leurs membres collectivement et par leurs propres moyens, ou qui poursuivent des buts politiques religieux, économiques, artistiques, d'intérêt général, sociaux ou analogues, pour autant que la banque constate que les buts énumérés ne sont pas les seuls à être poursuivis.

II. Ayant droit économique d'une société de domicile

- 40 L'ayant droit économique d'une société de domicile peut être soit une personne physique, soit une personne morale qui exerce une activité de commerce ou de fabrication ou une autre activité exploitée en la forme commerciale. Une société de domicile ne peut pas être elle-même ayant droit économique.
- 41 L'identification des ayants droit économiques doit être établie et conservée conformément aux ch. 27 CDB et 28. Le ch. 29 CDB est applicable.
- 42 Il n'y a pas lieu d'identifier les ayants droit économiques d'une société de domicile cotée en bourse.

- 43 Dans le cas de groupements de personnes ou d'entités patrimoniales pour lesquels il n'existe pas d'ayant droit économique déterminé (p. ex. les discretionary trusts), une déclaration écrite confirmant cet état de fait doit être exigée du cocontractant, en lieu et place de l'identification de l'ayant droit économique. Cette déclaration doit en outre indiquer le fondateur effectif (et non pas fiduciaire) ainsi que, si elles peuvent être déterminées, les personnes habilitées à donner des instructions au cocontractant ou à ses organes et le cercle des personnes pouvant entrer en ligne de compte comme bénéficiaires (par catégorie, p. ex. «membres de la famille du fondateur»). S'il existe des curateurs, des protecteurs, etc., ils doivent également figurer dans la déclaration.
- 44 Pour les constructions révocables (p. ex. les revocable trusts), le fondateur effectif doit être indiqué comme ayant droit économique.

III. Modification des signatures autorisées

- 45 Si des changements interviennent dans les signatures autorisées de la société de domicile dans ses relations avec la banque, cette dernière doit répéter la procédure prévue à l'art. 4, al. 2, lit. b CDB, à moins qu'il soit manifeste ou qu'elle n'obtienne confirmation écrite de la part des organes dirigeants de la société de domicile ou de ses signataires autorisés du fait que l'ayant droit économique n'a pas changé. Si la banque ne parvient pas à établir clairement qui est l'ayant droit économique, l'art. 6, al. 3 CDB est applicable.

Art. 5 Personnes tenues à un secret professionnel

Les banques peuvent renoncer à l'identification de l'ayant droit économique pour les comptes ou les dépôts établis au nom d'avocats ou de notaires autorisés à exercer en Suisse, pour le compte de leurs clients, dans la mesure où, selon une déclaration écrite de

l'avocat ou du notaire, les comptes et les dépôts concernés ne servent qu'à l'un des buts suivants expressément reconnaissable (nature du mandat):

- a) – paiement d'avances ou de frais de procédure, de sûretés, de contributions de droit public, etc., versements en faveur ou de la part d'une partie, de tiers ou d'une autorité, ainsi que, dans la mesure appropriée, les placements à court terme qui leur sont liés, (libellé p. ex. «avoirs de clients – compte/dépôt de passage»);
- b) – dépôt de valeurs patrimoniales ainsi que, dans la mesure appropriée, les placements qui lui sont liés, relatif à un partage successoral en cours ou à l'exécution de dispositions à cause de mort (libellé p. ex. «succession» ou «partage successoral»);
 - dépôt/placement de valeurs patrimoniales relatif à la liquidation en cours d'un régime matrimonial dans le cadre d'un divorce ou d'une séparation (libellé p. ex. «liquidation de régime matrimonial/divorce»);
 - dépôt/placement à titre de sûretés de valeurs patrimoniales dans le cadre d'affaires de droit civil ou de droit public (libellé p. ex. «compte/dépôt escrow», «dépôt bloqué pour achat d'actions», «dépôt à titre de sûreté d'une caution de l'entrepreneur», «dépôt à titre de sûreté, impôt sur les bénéfices immobiliers», etc.);
 - dépôt de valeurs patrimoniales ainsi que, dans la mesure appropriée, les placements qui lui sont liés, dans le cadre de procédures de droit civil ou de droit public devant les tribunaux ordinaires ou arbitraux, ainsi que dans le cadre de procédures d'exécution forcée (libellé p. ex. «provisions», «garantie caution judiciaire», «masse en faillite», «procédure arbitrale», etc.).

disponible en français, allemand et italien auprès du secrétariat de l'Association suisse des banquiers, à Bâle.

² Les formulaires que les banques peuvent établir selon leurs besoins particuliers doivent contenir le texte intégral du formulaire modèle (voir annexe).

Art. 6 Modifications ou défauts en relation avec la vérification de l'identité du cocontractant ou l'identification de l'ayant droit économique (art. 2-5 CDB)

¹ La banque doit répéter la procédure prévue aux articles 2, ch. 9-24, et articles 3 et 4, ch. 25-45 CDB

- lorsque dans le courant des relations d'affaires, un doute survient
 - au sujet de l'exactitude des indications données sur l'identité du cocontractant
 - sur le point de savoir si le cocontractant est lui-même l'ayant droit économique, ou
 - sur le point de savoir si la déclaration remise au sujet de l'ayant droit économique est conforme à la réalité;
- lorsque des indices de modifications survenues a posteriori existent.

² Lorsqu'une banque constate qu'une déclaration au sens de l'art. 5 CDB a été établie à tort, elle doit exiger de son cocontractant l'identification de l'ayant droit économique au moyen d'un formulaire A. Si la déclaration relative à l'ayant droit économique n'est pas fournie, les relations d'affaires doivent être rompues.

³ Les banques sont tenues de rompre leurs relations avec le cocontractant lorsque les opérations effectuées laissent soupçonner que la banque a été trompée lors de la vérification de l'identité du cocontractant, lorsque des indications sciemment erronées lui ont été données à propos de l'ayant droit économique ou lorsque des doutes subsistent au sujet des indications fournies par le co-

contractant après que la procédure visée à l'al. 1 a été menée à bien.

⁴ Les relations avec le cocontractant ne peuvent plus être rompues lorsque les conditions de l'obligation de communiquer (art. 9 LBA) sont remplies.

- 47 Les relations existantes doivent être rompues aussi rapidement qu'il est possible de le faire sans violer le contrat. Si la banque n'est pas en mesure d'atteindre le cocontractant, en raison des instructions reçues en matière de correspondance, elle peut attendre pour rompre les relations d'affaires la prochaine visite de ce dernier ou la prochaine remise de correspondance.

B Interdiction de l'assistance active à la fuite de capitaux

Art. 7 *Fuite de capitaux*

Les banques ne doivent prêter aucune assistance active au transfert de capitaux hors des pays dont la législation prévoit des restrictions en matière de placement de fonds à l'étranger.

- 48 ¹ La fuite de capitaux est un transfert non autorisé de capitaux effectué sous la forme de devises, de billets de banque ou de papiers-valeurs et provenant d'un pays qui interdit ou limite un tel transfert à l'étranger de la part de ses résidents.

² La simple obligation d'annonce lors de transferts de capitaux ne constitue pas une limite à la circulation de capitaux au sens de la convention.

- 49 L'art. 7 CDB n'est pas applicable au transfert de capitaux de Suisse à l'étranger.

- 50 Sont considérés comme assistance active:

- a) l'organisation de l'accueil de clients à l'étranger en dehors des propres locaux de la banque dans le but d'accepter des fonds;
- b) la participation, à l'étranger, à l'organisation d'opérations de compensation, lorsque la banque sait ou, d'après l'ensemble des circonstances, doit savoir que la compensation sert à la fuite de capitaux;
- c) la collaboration active avec des personnes ou sociétés qui organisent pour des tiers la fuite de capitaux ou apportent une aide à cet effet
 - en leur donnant des ordres;
 - en leur promettant des commissions;
 - en tenant leurs comptes lorsque la banque sait que ces personnes ou sociétés utilisent leurs comptes professionnellement en vue d'aider la fuite des capitaux;

- d) le fait de donner au client des indications sur des personnes et sociétés mentionnées sous lit. c.
- 51 Les visites rendues à des clients à l'étranger sont autorisées dans la mesure où le mandataire de la banque n'accepte pas de fonds dont le transfert est interdit, ne donne aucun conseil en vue du transfert illégal de capitaux, ni ne participe à des opérations de compensation.
- 52 Pour le surplus, les fonds de clients étrangers peuvent être acceptés en Suisse.

C Interdiction de l'assistance active à la soustraction fiscale et à des actes analogues

Art. 8 *Soustraction fiscale et actes analogues*

Les banques ne doivent pas fournir une aide à leurs clients dans des manœuvres visant à tromper les autorités suisses et étrangères, en particulier les autorités fiscales, au moyen d'attestations incomplètes ou pouvant induire en erreur d'une autre manière.

53 ¹ Il est interdit de délivrer au client lui-même ou, à sa demande, directement à des autorités suisses ou étrangères, des attestations incomplètes ou de nature à induire en erreur d'une autre manière.

² On entend par autorités, notamment, les autorités fiscales, douanières, monétaires et de surveillance des banques, ainsi que les autorités chargées des poursuites pénales.

54 ¹ Sont soumises à cette interdiction les attestations particulières demandées par le client à l'intention d'autorités.

² Les pièces justificatives établies régulièrement, telles qu'extraits de compte et de dépôt, avis de crédit et de débit, décomptes d'opérations de change, décomptes de coupons et de bourse, ne doivent pas être modifiées par la banque dans le but de tromper.

55 ¹ Les attestations sont incomplètes lorsque des faits significatifs sont omis en vue de tromper des autorités, par exemple lorsque la banque supprime, à la demande du client, une ou plusieurs positions dans une attestation particulière ou dans un extrait de compte ou de dépôt.

² Dans les extraits de compte ou de dépôt, il n'est pas nécessaire de mentionner que d'autres comptes ou dépôts sont tenus pour le même client.

56 Les attestations sont de nature à induire en erreur lorsque des faits

sont présentées de manière contraire à la vérité, en vue de tromper les autorités, par exemple:

- a) en indiquant des dates, des montants ou des cours qui ne correspondent pas à la réalité ou en établissant des avis de crédit ou de débit portant des indications fausses sur les titulaires des comptes;
- b) en attestant des créances ou des dettes fictives (sans égard au fait que l'attestation corresponde ou non aux livres de la banque);
- c) par la mise à disposition des propres comptes de la banque, dans la mesure où elle permet au client d'éluder des contributions fiscales dues.

D Autres dispositions

Art. 9 Comptes numérotés

Les dispositions de la présente convention s'appliquent sans aucune réserve aux comptes, livrets, dépôts et compartiments de coffre-fort désignés par un numéro ou un code.

- 57 Les comptes et dépôts numérotés ou désignés par un code, y compris les placements fiduciaires, doivent être inclus dans les attestations relatives à l'ensemble des relations d'affaires avec un client.

Art. 10 Contrôle par les organes de révision

¹ En adhérant à la présente convention, les banques chargent leurs organes de révision prévus par la loi sur les banques et leur donnent l'autorisation de vérifier par sondages, à l'occasion de la révision ordinaire des comptes, que les dispositions de la convention ont été respectées. Les organes de révision prévus par la Loi sur les banques communiquent à la Commission de surveillance instituée par l'art. 12 CDB et à la Commission fédérale des banques les infractions qu'ils constatent ou qu'ils peuvent légitimement soupçonner.

² L'Association suisse des banquiers transmet aux organes de révision agréés le texte de la présente convention ainsi que la liste des signataires. Elle leur transmet ainsi le mandat décrit.

Art. 11 Violation de la convention, sanctions

¹ En cas de violation de la convention, la banque fautive est tenue de verser à l'Association suisse des banquiers une amende conventionnelle allant jusqu'à 10 millions de francs. Lors de la fixation de l'amende conventionnelle, il est dûment tenu compte de la gravité de la violation, du degré de culpabilité et de la situa-

tion financière de la banque. Il est en outre tenu compte des mesures imposées par d'autres instances dans le même cas d'espèce. Le montant de l'amende conventionnelle est déterminé selon la procédure prévue aux art. 12 et 13 CDB. L'Association suisse des banquiers attribue le montant de l'amende conventionnelle à un but d'utilité publique choisi par elle, après avoir déduit le montant éventuellement nécessaire à la couverture des frais de fonctionnement.

² Dans les cas de peu de gravité, un blâme peut être adressé à la banque fautive en lieu et place d'une amende conventionnelle.

³ En cas de violation de l'art. 6 al. 1 et 2 CDB une peine conventionnelle ou un blâme ne sera prononcé qu'en présence d'une négligence grave, et, en cas de violation des articles 7 et 8 CDB, que s'il y a eu violation intentionnelle des dispositions précitées.

⁴ Les violations de la convention qui remontent à plus de 5 ans ne sont plus poursuivies. En cas de manquement à l'obligation de vérifier l'identité du cocontractant ou d'identifier l'ayant droit économique, le délai de 5 ans commence à courir lorsque le manquement a été réparé, respectivement au moment où les relations d'affaires ont pris fin.

Art. 12 Commission de surveillance, chargés d'enquête

¹ L'Association suisse des banquiers institue une Commission de surveillance, composée de cinq personnalités indépendantes, en vue d'établir et de réprimer les violations de la présente convention. La Commission de surveillance élit un secrétaire et définit ses tâches.

² L'Association suisse des banquiers désigne un ou plusieurs chargés d'enquête. Les chargés d'enquête requièrent de la Commission de surveillance l'ouverture de la procédure ainsi que le prononcé de la sanction, ou la suspension de l'enquête. Lorsqu'ils adressent une demande de renseignements à une banque, les

chargés d'enquête lui indiquent à quel titre elle est impliquée dans la procédure.

³ Les membres de la Commission de surveillance et les chargés d'enquête exercent leurs fonctions pendant une durée de cinq ans. La reconduction de leurs mandats est autorisée.

⁴ Si la Commission de surveillance constate une violation de la convention, elle prononce, dans la procédure contre la banque fautive, une sanction équitable, conformément à l'art. 11 CDB.

⁵ La Commission de surveillance règle la procédure et statue sur le paiement des frais.

⁶ Si la banque fautive se soumet à la décision de la Commission de surveillance, la procédure prend fin. A défaut, l'art. 13 CDB s'applique.

⁷ Si une banque refuse de participer aux actes d'enquête de la Commission de surveillance ou d'un chargé d'enquête, la Commission de surveillance peut prononcer une amende conventionnelle au sens de l'art. 11 CDB.

⁸ En tant que mandataires au sens de l'art. 47 de la Loi sur les banques, les membres de la Commission de surveillance, le secrétaire ainsi que les chargés d'enquête sont strictement tenus de garder le secret sur les faits dont ils ont eu connaissance durant la procédure. Les banques ne peuvent faire valoir le secret bancaire à l'égard de la Commission de surveillance ou d'un chargé d'enquête.

⁹ La Commission de surveillance informe la Commission fédérale des banques de ses décisions. Si elle devait constater l'existence d'abus de la part de détenteurs de secrets professionnels, la Commission de surveillance pourrait en outre en informer l'autorité disciplinaire concernée.

- 58 La Commission de surveillance informe périodiquement les banques et le public de sa jurisprudence en respectant le secret bancaire et le secret des affaires.

- 59 La Commission de surveillance peut - d'entente avec le Conseil d'administration de l'Association suisse des banquiers - donner aux banques une interprétation de la convention. Les banques adressent à l'Association suisse des banquiers, leurs demandes à ce propos.

Art. 13 Procédure arbitrale

¹ Si l'amende conventionnelle fixée par la Commission de surveillance n'est pas acquittée dans le délai imparti, un Tribunal arbitral, dont le siège est à Bâle, rendra, sur plainte de l'Association suisse des banquiers contre la banque concernée, une sentence définitive portant sur l'existence d'une violation de la Convention de diligence et, le cas échéant, sur l'amende conventionnelle à prononcer. A cet effet, les banques font élection de for à Bâle.

² L'Association suisse des banquiers et la banque nomment chacune un arbitre et les deux arbitres (ainsi désignés) nomment ensemble le sur-arbitre.

³ L'instance arbitrale est pendante dès le moment où l'Association suisse des banquiers a désigné l'arbitre qu'il lui appartient de nommer.

⁴ Si une partie n'a pas désigné son arbitre dans les 30 jours dès réception de la communication écrite de l'autre partie lui signifiant l'ouverture de la procédure d'arbitrage, ou si les deux arbitres ne sont pas parvenus à un accord sur la nomination du sur-arbitre dans les 30 jours suivant l'acceptation de leur mandat d'arbitre, le Tribunal d'appel («Appellationsgericht») du Canton de Bâle-Ville procédera, à la requête d'une partie, à la nomination.

⁵ Si un arbitre ne peut exercer ses fonctions pour une raison quelconque, la partie qui l'a désigné doit nommer un nouvel arbitre dans les 30 jours; à défaut, le Tribunal d'appel du Canton de Bâle-Ville procédera, sur demande de l'autre partie, à la nomination de l'arbitre.

⁶ Si le sur-arbitre ne peut exercer ses fonctions pour une raison quelconque, les deux arbitres doivent, à nouveau, nommer le sur-arbitre; à défaut d'accord entre eux, le Tribunal d'appel du Canton de Bâle-Ville procédera à la nomination, sur requête de l'une des parties.

⁷ En cas de remplacement d'un arbitre conformément aux al. 5 et 6 CDB, les actes de procédure auxquels ce dernier a participé demeurent valables.

⁸ Sous réserve des dispositions impératives du Concordat suisse sur l'arbitrage et du Code de procédure civile du Canton de Bâle-Ville, les dispositions de ces derniers ne s'appliquent que si les parties ou, à défaut, le Tribunal arbitral n'adoptent pas d'autres règles de procédure. Le principe selon lequel tous les faits et les moyens doivent être invoqués dès le début de la procédure ne s'applique, au plus tôt, que lors du deuxième échange d'écritures (dérogation à la «Eventualmaxime»).

⁹ Le Tribunal arbitral est soumis au même devoir de discrétion que celui prévu à l'art. 12, al. 8 CDB.

Art. 14 Entrée en vigueur

¹ La présente convention entre en vigueur le 1^{er} juillet 2003.

² L'Association suisse des banquiers et chaque banque signataire sont autorisées à dénoncer la présente convention moyennant un préavis de trois mois, pour la fin d'une année contractuelle, mais au plus tôt pour le 30 juin 2008.

³ L'Association suisse des banquiers se réserve le droit – après consultation de la Commission fédérale des banques ou à la requête de cette dernière – de porter à la connaissance des banques, des dispositions complémentaires pendant la durée de validité de la convention (cf. Art. 16 LBA).

⁴ L'Association suisse des banquiers se réserve le droit de modifier unilatéralement le système de sanctions (art. 11–13 CDB) ou de l'abroger, dans la mesure où de nouvelles prescriptions légales ou

l'évolution du droit conduiraient à une accumulation inéquitable de sanctions pour les mêmes faits.

Art. 15 Disposition transitoire

¹ Les nouveaux formulaires A doivent être utilisés lorsque de nouvelles relations d'affaires sont établies après l'entrée en vigueur de la présente convention, ou lorsque la procédure d'identification de l'ayant droit économique doit être répétée conformément à l'art. 6 CDB.

² Les nouvelles règles relatives à la vérification de l'identité du co-contractant et à l'identification de l'ayant droit économique doivent être appliquées aux nouvelles relations d'affaires établies après l'entrée en vigueur de la présente convention, ou lorsque la procédure d'identification de l'ayant droit économique doit être répétée conformément à l'art. 6 CDB. Les nouvelles dispositions s'appliquent aux relations d'affaires déjà existantes lorsqu'elles constituent un allègement par rapport aux anciennes règles.

A

N° du compte/dépôt:

Cocontractant:

Identification de l'ayant droit économique

(Formulaire A selon art. 3 et 4 CDB)

Le cocontractant déclare:

(indiquer par une croix ce qui convient)

- ☐ que le cocontractant est le seul ayant droit économique des valeurs patrimoniales
- ☐ que l'ayant droit économique/les ayants droit économiques des valeurs patrimoniales est/sont:

Nom, prénom (ou raison sociale), date de naissance, nationalité, Adresse/siège, Etat

Le cocontractant s'engage à communiquer spontanément les modifications à la banque.

Le fait de remplir intentionnellement ce formulaire de manière erronée est punissable (Art. 251 du Code pénal suisse, faux dans les titres, réclusion jusqu'à 5 ans ou emprisonnement).

Lieu et date

Signature du cocontractant

R

N° du compte/dépôt:

Cocontractant:

Libellé :

**Déclaration lors de l'ouverture d'un compte ou d'un dépôt
par un avocat ou un notaire suisse**

Le/La soussigné(e) déclare par la présente qu'il/elle exerce l'activité d'avocat*/de notaire* et est soumis(e) à la législation cantonale en la matière

Il/Elle déclare qu'il/elle n'est pas lui-même l'ayant droit économique des valeurs en compte ou en dépôt. Il/Elle atteste qu'il/elle est soumis(e), en ce qui concerne le compte/le dépôt susmentionné, **au secret professionnel protégé par la loi (art. 321 CPS) et que ce compte/ce dépôt sert exclusivement à l'un des buts suivants:**

☐ paiement d'avances ou de frais de procédure, de sûretés, de contributions de droit public, etc., versements en faveur ou de la part d'une partie, de tiers ou d'une autorité, ainsi que, dans la mesure appropriée, les placements à court terme qui leur sont liés (libellé p. ex. «avoirs de clients - compte/dépôt de passage»);

☐ dépôt de valeurs patrimoniales ainsi que, dans la mesure appropriée, les placements qui lui sont liés, relatif à un partage successoral en cours ou à l'exécution de dispositions à cause de mort (libellé p.ex. «succession» ou «partage successoral»);

dépôt de valeurs patrimoniales ainsi que, dans la mesure appropriée, les placements qui lui sont liés, relatif à la liquidation en cours d'un régime matrimonial dans le cadre d'un divorce ou d'une séparation (libellé p. ex. «liquidation du régime matrimonial/divorce»);

dépôt à titre de sûretés ainsi que, dans la mesure appropriée, les placements qui lui sont liés, de valeurs patrimoniales dans le cadre d'affaires de droit civil ou de droit public (libellé p. ex. «compte/dépôt escrow», «dépôt bloqué pour achat d'actions», «dépôt à titre de sûreté d'une caution de l'entrepreneur», «dépôt à titre de sûreté, impôt sur les bénéfices immobiliers», etc.);

dépôt de valeurs patrimoniales ainsi que, dans la mesure appropriée, les placements qui lui sont liés, dans le cadre de procédures de droit civil ou de droit public devant les tribunaux ordinaires ou arbitraux, ainsi que dans le cadre de procédures d'exécution forcée (libellé p.ex. «provisions», «garantie caution judiciaire», «masse en faillite», «procédure arbitrale», etc).

(Indiquer par une croix ce qui convient; **une seule** rubrique peut être cochée).

Lieu et date

Signature

*Biffer ce qui ne convient pas

Le fait de remplir intentionnellement ce formulaire de manière erronée est punissable (Art. 251 du Code pénal suisse, faux dans les titres, réclusion jusqu'à 5 ans ou emprisonnement).

Versione del 10 febbraio 2003

**Convenzione
relativa all'obbligo di diligenza delle banche
(CDB 03)**

tra

l'Associazione Svizzera dei Banchieri

da una parte

e

le sottoscritte banche («banche»)

dall'altra parte

del 2 dicembre 2002

Introduzione

Art. 1 Premessa

- Allo scopo di salvaguardare la buona reputazione del sistema bancario svizzero all'interno e all'estero,
- nell'intento di definire delle norme che assicurino una irreprensibile gestione degli affari nell'accettazione di relazioni d'affari e nell'uso del segreto bancario,
- con la volontà di fornire un apporto efficiente alla lotta contro il riciclaggio di denaro e il finanziamento del terrorismo,

le banche si obbligano, con la firma della presente convenzione di diligenza, nei confronti dell'Associazione Svizzera dei Banchieri, nella sua qualità di organizzazione mantello incaricata di salvaguardare gli interessi e la reputazione del sistema bancario svizzero, a:

- a) identificare il loro contraente e farsi rilasciare da lui, nei casi dubbi, una attestazione riguardante l'avente diritto economico dei valori patrimoniali;
- b) non prestare alcuna assistenza attiva alla fuga di capitali;
- c) non prestare alcuna assistenza attiva all'evasione fiscale e ad atti simili rilasciando attestazioni incomplete o che in altro modo possano indurre in errore.

- 1 ¹ Sottostanno alla convenzione di diligenza le banche firmatarie con le loro sedi, succursali e agenzie stabilite in Svizzera, ma non le loro succursali, rappresentanze e società affiliate stabilite all'estero (cfr. però le cifre 11, 19 e 21).

² Le banche non possono in ogni caso ricorrere alle loro succursali estere o a società associate estere attive nel settore bancario o finanziario al fine di eludere la presente convenzione.

- 2 La convenzione di diligenza non modifica nulla quanto all'obbligo di salvaguardare il segreto bancario. Essa non può e non vuole:
- integrare le legislazioni: valutaria, fiscale ed in materia econo-

- mica estera nel diritto svizzero, né imporne l'osservanza alle banche svizzere (sempre che ciò non sia già previsto dai trattati internazionali in vigore e dalla legislazione svizzera);
- scostarsi dalla prassi giudiziaria attuale nel campo del diritto internazionale;
 - modificare lo status dei rapporti di diritto civile esistenti fra la banca e i suoi clienti.
- 3 La convenzione di diligenza rende vincolanti le regole di deontologia professionale della gestione bancaria. Esse mirano a concretizzare determinati doveri di diligenza regolamentati nell'ambito della legge sul riciclaggio di denaro (art. 3 – 5 LRD) così come il concetto di «diligenza richiesta dalle circostanze» nell'accettazione di valori patrimoniali (art. 305^{ter} CPS)¹. Gli obblighi particolari di chiarimento nell'ambito di relazioni d'affari o di transazioni ad alto rischio sono oggetto dell'ordinanza antiriciclaggio della CFB.
- Pertanto attraverso essa non deve essere intralciata la normale attività bancaria.

¹ L'applicazione per analogia della CDB agli emittenti delle carte di credito è disciplinata separatamente da specifiche norme.

A Identificazione del contraente e determinazione dell'avente diritto economico

Art. 2 Identificazione del contraente

¹ Le banche sono obbligate ad identificare il contraente al momento dell'apertura dei rapporti d'affari con lui.

² Ciò si applica per:

- l'apertura di conti o di libretti;
- l'apertura di depositi;
- l'espletamento di operazioni fiduciarie;
- la locazione di cassette di sicurezza;
- l'accettazione di mandati per amministrare patrimoni depositati presso terze persone;
- l'esecuzione di affari commerciali tramite titoli, divise così come metalli preziosi e altre merci (commodities) di importo superiore a fr. 25 000.–;
- le operazioni di cassa di importo superiore a fr. 25 000.–.

I. Campo d'applicazione

- 4 L'obbligo di accertare l'identità sussiste, con riserva di quanto stabilito alla cifra 18 per: l'apertura di conti, libretti e depositi di qualsiasi genere e per la locazione di cassette di sicurezza, siano essi tenuti al nome del contraente o sotto cifra (art. 9).
- 5 Per libretti di risparmio al portatore è da identificare chi effettua versamenti o prelevamenti di importo superiore a fr. 25 000.–. È da evitare l'apertura di nuovi libretti di risparmio al portatore.
- 6 Per titoli devono intendersi titoli di credito unificati e adatti al commercio di massa, diritti non documentali con la stessa funzione (diritti di valore) e derivati (cfr. art. 2 let. a LBCVM). In questa categoria sono anche da considerare prodotti finanziari non standardizzati.

- 7 Per operazioni di cassa devono intendersi le operazioni eseguite in contanti allo sportello (cambio, acquisto e vendita di metalli preziosi, sottoscrizione di obbligazioni di cassa e di prestiti obbligazionari, vendita in contanti di assegni di viaggio, incasso in contanti di assegni, ecc.). Versamenti e prelevamenti in contanti in relazione a conti o libretti esistenti così come depositi o consegne di titoli garantiti in relazione a depositi esistenti non sono da intendersi come operazioni di cassa (rimane riservata la cifra 5).
- 8 ¹ Il contraente deve essere identificato anche quando esegue operazioni per importi inferiori al limite minimo (art. 2 cpv. 2, 6. e 7. trattino), se elude in modo manifesto l'obbligo di identificazione ripartendo gli importi in diverse transazioni (il cosiddetto «smurfing»).
- ² A prescindere dal limite minimo (art. 2 cpv. 2, 6. e 7. trattino) e dalle eccezioni previste alla cifra 18, il contraente deve essere sempre identificato quando vi sia il sospetto che i valori patrimoniali possano avere un'origine criminosa (art. 9 cpv. 1 LRD). Non si deve invece identificare il contraente quando la banca rifiuta un affare o di aprire una relazione d'affari.

II. Identificazione del contraente

1. Persone fisiche
- a) Quando il cliente si presenta di persona
- 9 Quando il cliente si presenta di persona, la banca accerta l'identità del contraente prendendo visione di un documento di legittimazione con fotografia (passaporto, carta d'identità, licenza di condurre et simili), che viene fotocopiato annotando i dati richiesti secondo la cifra 22.

- b) Quando i rapporti d'affari vengono aperti per corrispondenza
- 10 Quando i rapporti d'affari vengono aperti per corrispondenza oppure via Internet, la banca accerta l'identità del contraente richiedendo una copia autenticata di un documento di identificazione ai sensi della cifra 9 e la conferma dell'indirizzo del contraente mediante l'invio di corrispondenza o altro mezzo equivalente.
- 11 ¹ L'attestazione di autenticità della copia del documento di identificazione può essere rilasciata da
- a) una succursale, una rappresentanza o una società associata della banca,
 - b) una banca corrispondente o un altro intermediario finanziario che la banca emittente ha scelto per questo specifico scopo,
 - c) un notaio o un altro ente pubblico normalmente preposto al rilascio di tali attestazioni di autenticità.
- ² È considerata valida anche l'identificazione effettuata sulla base di un documento di legittimazione in occasione della consegna o del ritiro della corrispondenza, nella misura in cui vi sia la garanzia che la notifica postale giunga al destinatario e a lui solo.
2. Persone giuridiche e società
- a) con sede in Svizzera
- 12 La banca accerta se la ditta del contraente è iscritta al «Foglio ufficiale svizzero di commercio» o se la stessa è riportata in un sito web pubblico per le iscrizioni al registro di commercio (ad es. www.zefix.ch). La banca ha altresì facoltà di utilizzare elenchi e banche dati pubblicati da privati (Annuario svizzero del registro di commercio, ecc.). In caso negativo l'identità deve essere provata da un estratto del registro di commercio.
- 13 L'identità delle persone giuridiche e delle comunità di persone

non iscritte al registro di commercio (associazioni, fondazioni, comunioni di proprietà per piani, corporazioni e istituti autonomi di diritto pubblico) deve essere accertata in base agli statuti o ad altri documenti equivalenti.

b) con sede all'estero

- 14 L'accertamento dell'identità del contraente dev'essere stabilito in base a un estratto del registro di commercio, a un documento equivalente o in base a estratti di siti web pubblici per le iscrizioni al registro di commercio o documenti equivalenti, dai quali si può dedurre l'esistenza della persona giuridica o della società (ad es. «certificate of incorporation»).

c) disposizioni comuni

- 15 L'estratto del registro di commercio oppure il documento equivalente non deve essere datato di oltre 12 mesi. Un documento datato di oltre un anno può essere utilizzato insieme ad un attestato non più vecchio di 12 mesi dell'ufficio di revisione o a un «certificate of good standing».
- 16 In caso di identificazione di associazioni non iscritte nel registro di commercio va accertata e documentata anche l'identità di coloro che richiedono l'apertura della relazione, qualora abbiano diritto di firma.
- 17 ¹ Se l'identità della persona giuridica contraente è generalmente conosciuta, si può rinunciare alla procedura secondo le cifre 12 – 14. L'identità è da ritenere come generalmente conosciuta specialmente quando è una società aperta al pubblico oppure è legata in modo diretto o indiretto ad una simile. Se la banca rinuncia alla procedura secondo le cifre 12 – 14, il motivo è da registrare agli atti.

² La procedura semplificata secondo il cpv. 1 è inammissibile per società di sede, se queste non sono legate in modo diretto o indiretto ad una società aperta al pubblico.

3. Eccezioni

- 18 L'identità del contraente non deve essere formalmente accertata all'apertura
- a) di un conto, deposito o libretto a nome di un minorenni da parte di una terza persona maggiorenne, purché il versamento effettuato all'atto dell'apertura sia al massimo di fr. 25 000.-; in questo caso va accertata unicamente l'identità della persona maggiorenne che richiede l'apertura; la cifra 22 è applicabile per analogia; deve essere accertata l'identità del minorenni qualora egli stesso proceda all'apertura di un conto, deposito o libretto;
 - b) di un conto per garanzia di locazione relativo a un oggetto di locazione situato in Svizzera;
 - c) di un conto destinato al deposito degli importi relativi alla liberazione o all'aumento del capitale di una società anonima o di una società con garanzia limitata.
- 19 Se l'identità del contraente è già stata accertata in maniera equivalente all'interno del gruppo, non è necessario ripetere la procedura secondo le cifre 9 – 14. In questi casi, le unità del gruppo direttamente interessate devono disporre delle copie dei documenti d'identificazione originali. Sono fatti salvi i casi in cui le disposizioni di legge non ammettono tale trasferimento di dati.
- 20 Qualora, in via eccezionale, non risulti possibile identificare il contraente secondo le modalità prescritte, ad es. perché una persona non dispone di alcun documento d'identità o perché non è disponibile la documentazione necessaria relativa a una corpora-

zione o a un istituto di diritto pubblico, la banca ha facoltà di accertare l'identità in altro modo adeguato, consultando altri documenti probatori o richiedendo agli enti pubblici competenti le relative conferme o, per le persone giuridiche, l'ultimo attestato di un ufficio di revisione riconosciuto. Le conferme e le copie dei documenti sostitutivi vanno messe agli atti; inoltre, la circostanza eccezionale deve essere specificata in una nota informativa agli atti.

4. Disposizioni generali per l'accertamento dell'identità e per la sorveglianza

21 ¹ La banca può, mediante accordo scritto, delegare l'identificazione del contraente a persone o società, se

a) ha provveduto a istruirle in merito ai loro compiti e se

b) è in grado di controllare la corretta esecuzione dell'identificazione.

² La persona incaricata è tenuta a trasmettere gli atti di identificazione alla banca e ad attestare che le copie trasmesse sono conformi ai documenti originali.

³ È esclusa una sottodelega da parte della persona incaricata.

22 Devono essere opportunamente annotati: il nome, il cognome, la data di nascita, la nazionalità e l'indirizzo del luogo di domicilio rispettivamente la ragione sociale e la sede del contraente, come pure i documenti in base ai quali l'identità è stata accertata. In caso di contraenti provenienti da paesi in cui data di nascita e indirizzo di domicilio non vengono utilizzati, tali indicazioni sono superflue. Le fotocopie del documento ufficiale di legittimazione e gli altri documenti di identificazione devono essere conservati.

23 La banca deve garantire che l'organo di controllo interno e l'ufficio di revisione previsto dalla legge sulle banche siano posti in grado di poter verificare che l'accertamento dell'identità viene effettuato.

- 24 In linea di principio, prima di poter utilizzare un conto devono essere presentati, nella forma richiesta e debitamente compilati, tutti i documenti necessari all'identificazione. In via eccezionale, un conto può essere utilizzato anche prima a condizione che la banca predisponga un sistema di controllo che garantisca il ricevimento dei documenti mancanti entro 30 giorni. Non sono comunque ammessi prelevamenti su richiesta del cliente. Se a scadenza dei 30 giorni la documentazione risulta ancora incompleta, il conto viene bloccato. La banca è tenuta ad annullare la relazione d'affari se dopo 90 giorni la documentazione non è ancora completa (cfr. anche l'art. 6 cpv. 4).

Art. 3 Determinazione dell'avente diritto economico

¹ La banca deve determinare l'avente diritto economico usando la diligenza richiesta dalle circostanze. Quando sussistono dubbi sul fatto che il contraente coincida con l'avente diritto economico, le banche devono esigere dal contraente una dichiarazione scritta – usando il formulario A – con la quale egli attesti chi sia l'avente diritto economico.

² Questo vale per:

- l'apertura di conti o di libretti;
- l'apertura di depositi;
- l'espletamento di operazioni fiduciarie;
- l'accettazione di mandati per amministrare patrimoni depositati presso terze persone;
- l'esecuzione di affari commerciali tramite titoli, divise così come metalli preziosi e altre merci (commodities) di importo superiore a fr. 25 000.–.

³ Per le operazioni di cassa di importo superiore a fr. 25 000.–, ai sensi dell'art. 2, si deve sempre esigere una dichiarazione del contraente riguardante l'avente diritto economico. Le banche devono annotare le dichiarazioni del contraente in maniera adeguata. Per questi casi esse possono utilizzare il formulario A.

- 25 ¹ La banca è legittimata a presumere che il contraente si identifichi con l'avente diritto economico. Tuttavia la presunzione non sussiste quando ci si trovi di fronte a situazioni anomale.
- ² Sussistono dubbi nei seguenti casi:
- quando viene rilasciata procura in favore di una persona la quale, manifestamente, non ha rapporti sufficientemente stretti con il contraente (non rientrano in questa categoria le procure di amministrazione conferite agli intermediari finanziari);
 - quando la situazione finanziaria della persona che chiede di porre in essere una delle operazioni elencate all'art. 3 è nota alla banca ed i valori conferiti, o da conferire, superano tale situazione finanziaria;
 - o quando la banca rilevi, nel corso del rapporto con il cliente, delle circostanze insolite.
- 26 Quando i rapporti d'affari vengono aperti per corrispondenza con una persona fisica, si deve esigere in ogni caso la dichiarazione sul formulario A. Sono esclusi i casi elencati alla cifra 18.
- 27 Se il contraente dichiara che l'avente diritto economico è un terzo, egli deve annotarne il nome, il cognome, la data di nascita, la nazionalità, l'indirizzo e il paese di domicilio, oppure, se si tratta di una persona giuridica, la ragione sociale, l'indirizzo e la sede, utilizzando il formulario A. L'art. 3 cpv. 3 rimane riservato. Se l'avente diritto economico proviene da un paese in cui data di nascita e indirizzo di domicilio non vengono utilizzati, tali indicazioni sono superflue.
- 28 Il formulario A può essere firmato dal contraente o da un suo procuratore (con procura individuale o generale per iscritto). In caso di persone giuridiche, il formulario A o la procura devono essere firmati dalle persone con diritto di firma menzionate nella documentazione societaria.

- 29 Se rimangono seri dubbi sulla correttezza della dichiarazione scritta dal contraente, dubbi che non possono essere eliminati mediante ulteriori chiarimenti, la banca deve rifiutare l'assunzione dei rapporti d'affari o l'esecuzione dell'operazione.
- 30 Il formulario A è allegato alla presente convenzione di diligenza. Il formulario, in lingua tedesca, francese, italiana, spagnola e inglese è ottenibile presso il Segretariato dell'Associazione Svizzera dei Banchieri.
- 31 Le banche hanno la facoltà di fare stampare propri formulari che soddisfino i loro particolari bisogni. Tuttavia, questi formulari devono riprodurre integralmente il testo del formulario modello.
- 32 Per i conti e i depositi collettivi, il titolare del conto o del deposito deve consegnare alla banca una lista degli aventi diritto economico con le indicazioni previste alla cifra 27 e comunicarle immediatamente ogni suo cambiamento.
- 33 Per forme di investimento collettive e società di partecipazione con più di 20 aventi diritto economico come investitori, vanno accertate le indicazioni secondo la cifra 27 riguardo a quelli che da soli o in accordo comune hanno diritti sul capitale apportato nella misura di almeno il 5%. Fino a 20 aventi diritto economico le indicazioni secondo la cifra 27 devono essere accertate per tutti. Forme d'investimento collettive quotate in borsa non sono tenute a rilasciare alcuna dichiarazione riguardo all'appartenenza economica.
- 34 ¹ In linea di principio, le banche con sede in Svizzera o all'estero non devono rilasciare alcuna dichiarazione riguardo all'appartenenza economica. Per la definizione di banca valgono le leggi speciali del paese di domicilio. Vanno tuttavia richiesti chiarimenti ri-

guardo all'appartenenza economica quando una banca non soggetta ad un'adequata sorveglianza o regolamentazione nell'ambito della lotta contro il riciclaggio di denaro affida la gestione di sottoconti per clienti anonimi.

² Altri intermediari finanziari con sede rispettivamente domicilio in Svizzera non devono rilasciare alcuna dichiarazione riguardo all'appartenenza economica. Lo stesso vale per gli altri intermediari finanziari domiciliati all'estero che sono assoggettati ad un'adequata sorveglianza e regolamentazione nell'ambito della lotta contro il riciclaggio di denaro.

³ Per altri intermediari finanziari nazionali e stranieri sono da intendere: amministrazioni di fondi, società di assicurazione sulla vita, commercianti di valori mobiliari ed enti di previdenza professionale esenti da imposte ai sensi dell'art. 2 cpv. 2 LRD. Per la definizione di intermediario finanziario estero valgono le leggi speciali corrispondenti del paese di domicilio.

⁴ Se risultano abusi da parte di una banca o di un altro intermediario finanziario, oppure esistono raccomandazioni generali della Commissione federale delle banche o dell'Associazione Svizzera dei Banchieri su singoli istituti o su istituti di un determinato paese, allora bisogna raccogliere dichiarazioni riguardo all'appartenenza economica oppure adottare altri provvedimenti.

35 ¹ È possibile delegare a terzi la determinazione dell'avente diritto economico applicando, per analogia, in applicazione le disposizioni di cui all'art. 21.

² Per la determinazione dell'avente diritto economico è applicabile, per analogia, la cifra 24.

36 La banca deve garantire che l'organo di controllo interno e l'ufficio di revisione previsti dalla legge sulle banche siano posti in grado di verificare che venga effettuato l'accertamento dell'identità dell'avente diritto economico.

- 37 Restano riservate le norme speciali dettate per i soggetti sottoposti al segreto professionale e quelle relative alle società di sede (art. 4 e 5, cifre 38 – 46).

Art. 4 Procedura relativa alle società di sede

¹ Ai sensi della presente convenzione di diligenza si intendono società di sede: tutte le società, Anstalten, fondazioni, trusts/società fiduciarie, ecc., che non esercitano nello Stato dove sono domiciliate attività commerciale, di fabbricazione, o qualunque altra attività condotta in forma commerciale.

² Dalle società di sede sia svizzere che straniere, si devono esigere:

- a) ai fini dell'identificazione: un estratto del registro di commercio oppure un certificato ad esso equivalente (cfr. cifre 12 – 16);
- b) ai fini della determinazione dell'avente diritto economico: una dichiarazione del contraente, tramite formulario A, che attesti chi sia l'avente diritto economico dei valori patrimoniali.

³ Se la banca conosce l'avente diritto economico e dispone degli estremi secondo la cifra 27, può astenersi dal far ricorso al formulario A. Essa deve però annotare le sue informazioni nel dossier.

I. Società di sede

- 38 Indipendentemente dallo scopo, dalla funzione, dalla forma giuridica e dalla sede, le imprese (sia svizzere che straniere) sono considerate di sede quando
- a) non dispongono di uffici propri (sede presso un avvocato, una società fiduciaria, una banca, ecc.) oppure
 - b) non dispongono di proprio personale che operi esclusivamente per esse, oppure questo si occupa soltanto di lavori amministrativi (tenuta della contabilità, disbrigo della corrispondenza secondo le direttive che riceve dalle persone o dalle società che hanno l'effettivo dominio sulla società di sede).

- 39 Sono parimenti considerate società di sede le fondazioni di famiglia nonché altre persone giuridiche e società che perseguono lo scopo di salvaguardare, mediante un'azione comune, gli interessi dei propri membri o che si propongono un fine politico, religioso, scientifico, artistico, benefico, ricreativo (o simili), qualora la banca accerti che non vengono perseguiti unicamente tali obiettivi statutari.

II. Appartenenza economica a una società di sede

- 40 Avente diritto economico di una società di sede può essere tanto una persona fisica quanto una persona giuridica che esercita un'attività commerciale, di produzione oppure un'altra attività industriale gestita in forma commerciale. Una società di sede non può essere essa stessa l'avente diritto economico.
- 41 Gli aventi diritto economico devono essere determinati e annotati conformemente alla cifra 27 e 28. La cifra 29 è applicabile.
- 42 Se una società di sede è quotata in borsa, non è necessario determinarne gli aventi diritto economico.
- 43 Per le associazioni di persone o per le entità patrimoniali dove non esiste un avente diritto economico determinato (per es. i discretionary Trusts), al posto della determinazione dell'avente diritto economico da parte del contraente, si deve esigere una dichiarazione scritta che attesti questo stato di cose. La dichiarazione deve inoltre contenere indicazioni sui fondatori effettivi (e non quelli a titolo fiduciario) e, qualora fossero determinate, sulle persone abilitate a dare istruzioni al contraente o ai suoi organi, come pure sulla cerchia di persone che possono entrare in linea di conto quali beneficiarie (per categoria, ad es. «membri della famiglia del

fondatore»). Se esistono dei curatori, protettori, ecc., essi devono ugualmente figurare nella dichiarazione.

- 44 Per le strutture revocabili (ad es. revocable Trusts) il fondatore effettivo deve essere annotato come l'avente diritto economico.

III. Cambiamenti nelle firme autorizzate

- 45 Se intervengono cambiamenti nelle firme autorizzate della società di sede valide nell'ambito dei suoi rapporti con la banca, quest'ultima deve ripetere la procedura prevista dall'art. 4 cpv. 2 lett. b, salvo in quei casi dove sia chiaro oppure le venga confermato per iscritto dagli organi dirigenti della società di sede, o dai suoi aventi diritto di firma, che l'avente diritto economico non è cambiato. Se non è possibile individuare in modo chiaro l'appartenenza economica, si applica l'art. 6 cpv. 3.

Art. 5 Persone soggette al segreto professionale

Le banche possono astenersi dal determinare l'avente diritto economico per conti o depositi aperti per conto di clienti a nome di avvocati o notai autorizzati ad esercitare in Svizzera, purché l'avvocato o il notaio confermi con una dichiarazione scritta, che i conti o i depositi sono destinati esclusivamente a uno degli scopi seguenti così definiti (natura del mandato):

- a) – svolgimento di operazioni connesse con anticipazioni di spese giudiziali, cauzioni, oneri di diritto pubblico e così via, nonché con pagamenti destinati o provenienti dalle parti, da terzi o da autorità e, quando fosse compatibile con una delle operazioni sopraelencate, l'investimento a corto termine di questi capitali (rubrica «conto/deposito per il movimento di fondi clienti»);
- b) – deposito e, quando fosse compatibile con una delle operazioni qui sottoelencate, l'investimento di valori patrimoniali ine-

renti una divisione ereditaria o una esecuzione testamentaria in corso (rubrica ad es. «pratica ereditaria» o «divisione ereditaria»);

- deposito/investimento di valori patrimoniali inerenti una liquidazione del regime dei beni matrimoniali in corso nell'ambito di un divorzio o di una separazione (rubrica ad es. «liquidazione del regime dei beni matrimoniali per divorzio»);
- deposito/investimento di valori patrimoniali a titolo di garanzia connessi con pratiche in corso secondo il diritto civile o pubblico (rubrica ad es. «conto/deposito Escrow», «deposito bloccato per acquisto di azioni», «deposito in garanzia per una cauzione dell'imprenditore», «deposito in garanzia per le imposte sul maggior valore immobiliare», ecc.);
- deposito e, quando fosse compatibile con una delle operazioni qui sottoelencate, l'investimento di valori patrimoniali connessi con pratiche in corso secondo il diritto civile o pubblico davanti ai tribunali ordinari o arbitrali e nella procedura di esecuzione forzata (rubrica ad es. «anticipazioni», «garanzia per cauzione giudiziaria», «massa fallimentare», «procedura arbitrale», ecc.).

46 ¹ Il formulario R, che è da usare per la dichiarazione giusta l'art. 5, può essere richiesto in lingua tedesca, francese e italiana al Segretariato dell'Associazione Svizzera dei Banchieri a Basilea.

² I formulari stampati dalle banche secondo i loro bisogni particolari devono riprodurre integralmente il testo del formulario modello (vedi allegato).

Art. 6 Cambiamenti o carenze in relazione all'identificazione del contraente o nella determinazione dell'avente diritto economico (art. 2 – 5)

¹ La banca deve ripetere la procedura prevista agli art. 2 cifre 9 – 24, art. 3 e 4 cifre 25 – 45,

- quando nel corso delle relazioni d'affari sorgono dubbi,
 - riguardanti l'esattezza delle indicazioni date sull'identità del contraente,
 - se il contraente sia lui stesso l'avente diritto economico, o
 - se la dichiarazione riguardante l'avente diritto economico corrisponde alla realtà,
- quando esistono indizi di cambiamenti intervenuti posteriormente.

² Quando una banca constata che una dichiarazione ai sensi dell'art. 5 di questa convenzione di diligenza è stata utilizzata non a proposito, deve esigere dal contraente la dichiarazione per la determinazione dell'avente diritto economico, facendo compilare il formulario A. Se non viene fornita la dichiarazione riguardante l'avente diritto economico si devono interrompere le relazioni d'affari.

³ Le banche hanno l'obbligo di porre termine ai rapporti con il contraente quando, nel corso degli stessi, sorgesse il sospetto che la banca sia stata ingannata nell'accertamento dell'identità del contraente, che fossero state fornite intenzionalmente delle false indicazioni riguardanti l'avente diritto economico, o quando continuassero a sussistere dubbi sulle indicazioni del contraente, anche dopo aver seguito la procedura secondo il cpv. 1.

⁴ Le relazioni con il contraente non devono più essere interrotte quando i presupposti dell'obbligo di notifica (art. 9 LRD) sono soddisfatti.

- 47 Ai rapporti in essere deve essere posto termine il più rapidamente possibile senza violare il contratto. Se la banca in base alle istruzioni ricevute per l'invio della corrispondenza non fosse in grado di contattare il contraente, essa potrà attendere a porre termine ai rapporti fino alla prossima visita, oppure fino al prossimo invio della corrispondenza.

B Divieto di prestare assistenza attiva alla fuga di capitali

Art. 7 *Fuga di capitali*

Le banche non devono prestare alcuna assistenza attiva al trasferimento di capitali da paesi la cui legislazione ne limita il collocamento all'estero.

48 ¹ La fuga di capitali è un trasferimento non autorizzato di capitali sotto forma di divise, banconote o cartevalori, da un paese che vieta o limita a carico dei residenti tale trasferimento all'estero.

² Il semplice obbligo di notifica relativo all'esportazione di divise non è considerato una limitazione alla circolazione dei capitali.

49 L'art. 7 non si applica al trasferimento di capitali dalla Svizzera all'estero.

50 Sono forme di assistenza attiva

- a) l'organizzare incontri con clienti all'estero, fuori dai locali della banca, allo scopo di ricevere fondi;
- b) la partecipazione all'organizzazione all'estero di operazioni di compensazione, quando la banca sa, o dovrebbe sapere in base alle circostanze date, che la compensazione è strumentale alla fuga di capitali;
- c) la collaborazione attiva con persone e società che organizzano per conto di terzi la fuga di capitali, o prestano servizi a questo fine:
 - passando loro ordini,
 - promettendo loro provvigioni,
 - tenendo i loro conti quando alla banca è noto che tali persone e società utilizzano i loro conti allo scopo professionale di aiutare la fuga di capitali,
- d) il fatto di dare al cliente informazioni sulle persone e società di cui è detto sub c).

- 51 Le visite ai clienti all'estero sono autorizzate, purché l'incaricato della banca non accetti fondi il cui trasferimento è vietato, non dia consigli per il trasferimento illegale dei capitali, né partecipi a operazioni di compensazione.
- 52 Per il resto, i fondi di clienti esteri possono essere accettati in Svizzera.

C Divieto di prestare assistenza attiva all'evasione fiscale e ad atti simili

Art. 8 Evasione fiscale e atti simili

Le banche non devono favorire le manovre fraudolente dei loro clienti nei confronti delle autorità svizzere o straniere, in particolare le autorità fiscali, mediante attestazioni incomplete o che in altro modo possano indurre in errore.

53 ¹ È vietato il rilascio di attestazioni incomplete, o che in altro modo possano indurre in errore, al cliente stesso o, a sua richiesta, direttamente ad autorità svizzere o straniere.

² Per autorità si intendono in particolare le autorità fiscali, gli uffici doganali, le autorità valutarie e di vigilanza sulle banche come pure le autorità incaricate dell'istruzione del procedimento penale.

54 ¹ Sono colpite dal divieto le attestazioni particolari che il cliente richiede per fornirle alle autorità.

² Le attestazioni consuete, quali estratti conto e di deposito, gli avvisi di accredito e di addebito, i conteggi per operazioni in divisa, i conteggi per le cedole e per le operazioni di borsa, non devono essere modificati dalla banca in modo da consentire manovre fraudolente.

55 ¹ Le attestazioni sono incomplete quando, allo scopo di ingannare le autorità, vengono omessi fatti rilevanti, ad es. quando la banca, a richiesta del cliente, in una attestazione speciale o in un estratto conto o di deposito omette una o più posizioni.

² Negli estratti conto o di deposito non è necessario indicare che per il medesimo cliente sono aperti altri conti o depositi.

56 Le attestazioni possono indurre in errore quando, allo scopo di in-

ganno delle autorità, si espongono fatti in forma non vera ad es. mediante:

- a) date false, importi falsi, corsi fittizi od indicazione falsa dei destinatari di accrediti e di addebiti;
- b) attestazioni di crediti o debiti fittizi (indipendentemente dal fatto che l'attestazione corrisponda o meno alle registrazioni della banca);
- c) messa a disposizione di conti di proprietà della banca in modo che il cliente ottenga una riduzione degli oneri fiscali dovuti.

D Altre disposizioni

Art. 9 Conti cifrati

Le disposizioni della presente convenzione di diligenza si applicano integralmente ai conti, ai libretti, ai depositi ed alle cassette di sicurezza tenuti sotto cifra o sotto sigla.

- 57 Nelle dichiarazioni relative alla totalità dei rapporti d'affari con un cliente, devono essere inclusi anche i conti e depositi tenuti sotto cifra o sotto sigla, nonché gli investimenti fiduciari.

Art. 10 Controllo da parte degli organi di revisione

¹ Sottoscrivendo la presente convenzione di diligenza, le banche incaricano ed autorizzano i loro organi di revisione previsti dalla legge sulle banche a controllare per campione, durante la revisione ordinaria dei conti, l'osservanza della convenzione e comunicare alla commissione di sorveglianza prevista dall'art. 12, nonché alla Commissione federale delle banche, le infrazioni e i fondati dubbi d'esistenza di infrazioni.

² L'Associazione Svizzera dei Banchieri porterà a conoscenza dei competenti organi di revisione il testo della presente convenzione di diligenza, nonché la lista dei firmatari, allo scopo di informarli del mandato loro conferito.

Art. 11 Infrazioni alla convenzione di diligenza, sanzioni

¹ In caso di infrazione alla convenzione di diligenza, la banca che l'ha commessa deve versare una pena convenzionale all'Associazione Svizzera dei Banchieri che può elevarsi fino a 10 milioni di franchi. Nel determinare la pena convenzionale viene tenuto debitamente conto della gravità dell'infrazione, del grado di colpa e della situazione finanziaria della banca. Oltre a ciò si deve tenere conto dei provvedimenti inflitti da altre istanze nello stesso caso.

L'ammontare della pena convenzionale viene stabilito secondo la procedura prevista all'art. 12 o, se necessario, secondo quella di cui all'art. 13. Previa copertura dell'eventuale disavanzo risultante dal conteggio dei costi, l'Associazione Svizzera dei Banchieri devolve l'ammontare della pena convenzionale per scopi di pubblica utilità di sua scelta.

² Nei casi di lieve entità, in sostituzione della pena convenzionale può essere emessa una nota di biasimo a carico della banca che ha commesso l'infrazione.

³ Viene pronunciata una pena convenzionale rispettivamente una nota di biasimo soltanto se le infrazioni contro l'art. 6 cpv. 1 e 2 sono state commesse per colpa grave, o se le infrazioni contro gli art. 7 e 8 sono state commesse intenzionalmente.

⁴ Infrazioni alla convenzione di diligenza che risalgono ad oltre 5 anni non sono più perseguibili. In caso di violazione dell'obbligo di identificazione del contraente e dell'accertamento dell'avente diritto economico, il termine di 5 anni decorre dal momento in cui si è posto rimedio alla violazione, rispettivamente dal momento in cui sono state interrotte le relazioni d'affari.

Art. 12 Commissione di sorveglianza, inquirenti

¹ Per stabilire e punire le infrazioni alla presente convenzione di diligenza, l'Associazione Svizzera dei Banchieri istituisce una commissione di sorveglianza, composta da cinque personalità indipendenti. La commissione di sorveglianza elegge un segretario e definisce i suoi compiti.

² L'Associazione Svizzera dei Banchieri designa uno o più inquirenti. Gli inquirenti propongono alla commissione di sorveglianza l'apertura del procedimento e la pronuncia di una sanzione adeguata, oppure la sospensione dell'inchiesta. Nell'indirizzare le loro richieste d'informazione alla banca essi devono specificare il titolo per il quale essa è chiamata in causa.

³ I membri della commissione di sorveglianza e gli inquirenti restano in carica cinque anni. Il rinnovo del mandato è permesso.

⁴ Constatata l'infrazione alla convenzione di diligenza, la commissione di sorveglianza infligge, nel procedimento instaurato a carico della banca rea, la sanzione adeguata conformemente all'art. 11.

⁵ La commissione di sorveglianza stabilisce la procedura e determina a chi verranno accollate le spese.

⁶ Se la banca rea dell'infrazione si sottomette alla decisione della commissione di sorveglianza il procedimento prende fine. In caso contrario si applica l'art. 13.

⁷ Se la banca rifiuta di collaborare alle indagini della commissione di sorveglianza o di un inquirente, la commissione di sorveglianza può infliggere una pena convenzionale ai sensi dell'art. 11.

⁸ Quali persone che ricevono legittimazione dall'art. 47 della legge sulle banche, i membri della commissione di sorveglianza, il segretario e la/le persona/e incaricata/e dell'inchiesta devono mantenere un rigoroso segreto sui fatti venuti a loro conoscenza durante il procedimento. Le banche non possono far valere il segreto bancario nei confronti della commissione di sorveglianza o di un inquirente.

⁹ La commissione di sorveglianza comunica le proprie decisioni alla Commissione federale delle banche. Se vengono constatati abusi da parte di detentori del segreto professionale la commissione di sorveglianza può inoltre darne notizia alla competente autorità disciplinare.

- 58 La commissione di sorveglianza, rispettando il segreto bancario e quello degli affari, informa periodicamente le banche e l'opinione pubblica sulla prassi adottata nelle sue decisioni.
- 59 La commissione di sorveglianza può, d'intesa con il consiglio di amministrazione dell'Associazione Svizzera dei Banchieri, emana-

re all'attenzione delle banche norme interpretative della convenzione di diligenza. Le banche presentano le loro eventuali richieste in materia all'Associazione Svizzera dei Banchieri.

Art. 13 Procedura arbitrale

¹ Se la pena convenzionale, fissata in modo adeguato dalla commissione di sorveglianza, non è pagata nel termine stabilito, un tribunale arbitrale con sede a Basilea, su denuncia dell'Associazione Svizzera dei Banchieri contro la banca in questione, decide definitivamente: sull'esistenza di una trasgressione della convenzione di diligenza e, se necessario, sulla pena convenzionale da infliggere. Per questo scopo le banche eleggono il foro giudiziario a Basilea.

² L'Associazione Svizzera dei Banchieri e la banca designano ciascuna un arbitro. Successivamente i due arbitri così eletti designano insieme il presidente del tribunale arbitrale.

³ La procedura arbitrale è aperta con la designazione da parte dell'Associazione Svizzera dei Banchieri dell'arbitro di sua competenza.

⁴ Nel caso in cui una parte non abbia designato l'arbitro entro trenta giorni dal ricevimento della comunicazione scritta dell'altra parte riguardante l'apertura della procedura arbitrale, o nel caso in cui i due arbitri non si accordino sulla scelta del presidente del tribunale arbitrale entro trenta giorni dall'accettazione del mandato di arbitro, il Tribunale di appello («Appellationsgericht») del Cantone Basilea-Città, su richiesta di una parte, provvederà alla nomina.

⁵ Se un arbitro non potesse esercitare le sue funzioni per una qualsiasi ragione, la parte che lo ha designato dovrà nominare un nuovo arbitro entro trenta giorni. Altrimenti il Tribunale di appello del Cantone di Basilea-Città provvederà alla nomina, su richiesta dell'altra parte.

⁶ Se il presidente del tribunale arbitrale non potesse esercitare le

sue funzioni per una qualsiasi ragione, gli arbitri dovranno designare un nuovo presidente, entro trenta giorni. Altrimenti il Tribunale di appello del Cantone di Basilea-Città provvederà alla nomina, su richiesta di una parte.

⁷ In caso di sostituzione di un arbitro conformemente all'art. 13 cpv. 5 e 6, gli atti procedurali ai quali ha partecipato l'arbitro sostituito permarranno validi.

⁸ Riservate le norme imperative contrarie del concordato svizzero sull'arbitrato e del codice di procedura civile del Cantone di Basilea-Città, si applicano le disposizioni ivi dettate, a meno che le parti, o in loro difetto il tribunale arbitrale, non abbiano stabilito altre regole di procedura. La produzione dei mezzi di azione e di difesa (massima eventuale) deve avvenire al più tardi con il secondo scambio degli allegati scritti.

⁹ Anche il tribunale arbitrale è obbligato a rispettare il dovere di discrezione di cui all'art. 12 cpv. 8.

Art. 14 Entrata in vigore

¹ La presente convenzione di diligenza entra in vigore il 1° luglio 2003.

² L'Associazione Svizzera dei Banchieri e ciascuna banca firmataria potranno recedere dalla presente convenzione di diligenza mediante preavviso di tre mesi per la fine di ogni anno contrattuale, ma non prima del 30 giugno 2008.

³ Previo accordo con la Commissione federale delle banche o su richiesta della stessa (cfr. art. 16 LRD), l'Associazione Svizzera dei Banchieri si riserva il diritto di notificare alle banche eventuali disposizioni integrative per l'intera durata della convenzione.

⁴ L'Associazione Svizzera dei Banchieri si riserva il diritto di modificare unilateralmente o di abrogare il sistema delle sanzioni (art. 11 – 13), qualora nuove disposizioni legali o l'evoluzione del diritto condurrebbero a punire i medesimi fatti con più sanzioni e in modo iniquo.

Art. 15 Disposizioni transitorie

¹ I nuovi formulari A sono da utilizzare quando, dopo la data di entrata in vigore della convenzione di diligenza, vengono aperte nuove relazioni d'affari o si deve ripetere la procedura per la determinazione dell'avente diritto economico ai sensi dell'art. 6.

² La nuova regolamentazione sull'identificazione del contraente e sulla determinazione dell'avente diritto economico è da applicare all'apertura di una nuova relazione d'affari dopo la data dell'entrata in vigore della presente convenzione di diligenza oppure quando la procedura per la determinazione dell'avente diritto economico secondo l'art. 6 sia da ripetere dopo l'entrata in vigore della presente convenzione di diligenza. Per relazioni d'affari in vigore, le nuove regole sono da applicare solo nel caso esse siano più favorevoli.

A

No. del conto/del deposito:

Contraente:

Determinazione dell'avente diritto economico

(Formulario A conformemente agli art. 3 e 4 CDB)

Con la presente il contraente dichiara:

(indicare con una croce ciò che fa al caso)

☐ che il contraente, e lui solo, è l'avente diritto economico dei valori patrimoniali☐ che l'avente/gli aventi diritto economico dei valori patrimoniali è/sono:

nome, cognome/o ragione sociale, data di nascita, nazionalità, indirizzo/sede, Stato

Il contraente si obbliga a comunicare volontariamente ogni cambiamento alla banca.

La compilazione intenzionalmente falsa del presente formulario è punibile (art. 251 del Codice penale svizzero, falsità in documenti; pena prevista: reclusione sino a cinque anni o detenzione).

Luogo e data

Firma del contraente

R

No. del conto/del deposito:

Contraente:

Rubrica:

**Dichiarazione all'atto dell'apertura di un conto o di un deposito da parte
di un avvocato o di un notaio svizzero**

Con la presente il/la sottoscritto/a dichiara di agire in qualità di avvocato/notaio* e di essere assoggettato alla legislazione cantonale in materia.

Egli/ella dichiara di non essere lui/lei stesso/a l'avente diritto economico dei valori che vengono depositati di volta in volta. Egli/ella attesta che, per quel che concerne i conti/depositi sopramenzionati, **è assoggettato/a al segreto professionale (art. 321 CPS) e che questi conti/depositi sono destinati esclusivamente a uno degli scopi seguenti:**

☐ lo svolgimento di operazioni connesse con anticipazioni di spese giudiziali, cauzioni, oneri di diritto pubblico e così via, nonché con pagamenti destinati o provenienti dalle parti, da terzi o da autorità e, quando fosse compatibile con una delle operazioni sopraelencate, l'investimento a corto termine di questi capitali (rubrica «conto/deposito per il movimento di fondi clienti»);

☐ il deposito e, quando fosse compatibile con una delle operazioni sottoelencate, l'investimento di valori patrimoniali inerenti una divisione ereditaria o una esecuzione testamentaria in corso (rubrica ad es. «pratica ereditaria» o «divisione ereditaria»);

il deposito e, quando fosse compatibile con una delle operazioni sottoelencate, l'investimento di valori patrimoniali inerenti una liquidazione del regime dei beni matrimoniali in corso nell'ambito di un divorzio o di una separazione (rubrica ad es. «liquidazione del regime dei beni matrimoniali per divorzio»);

il deposito e, quando fosse compatibile con una delle operazioni sottoelencate, l'investimento di valori patrimoniali a titolo di garanzia connessi con pratiche in corso secondo il diritto civile o pubblico (rubrica ad es. «conto/deposito Escrow», «deposito bloccato per acquisto di azioni», «deposito in garanzia per una cauzione dell'imprenditore», «deposito in garanzia per le imposte sul maggior valore immobiliare», ecc.);

il deposito e, quando fosse compatibile con una delle operazioni sottoelencate, l'investimento di valori patrimoniali connessi con pratiche in corso secondo il diritto civile o pubblico davanti ai tribunali ordinari o arbitrali e nella procedura di esecuzione forzata (rubrica ad es. «anticipazioni», «garanzia per cauzione giudiziaria», «massa fallimentare», «procedura arbitrale», ecc.).

(Contrassegnare il riquadro che interessa. È consentito contrassegnare **un solo** riquadro).

Luogo e data

Firma

*Cancellare ciò che non fa al caso

La compilazione intenzionalmente falsa del presente formulario è punibile (art. 251 del Codice penale svizzero, falsità in documenti; pena prevista: reclusione sino a cinque anni o detenzione).

Version February 10, 2003

**Agreement
on the Swiss banks' code of conduct with regard
to the exercise of due diligence
(CDB 03)**

between

The Swiss Bankers Association

on the one hand

and

The signatory banks (hereinafter "the banks")

on the other hand

of December 2, 2002

Introduction

Art. 1 Preamble

- With a view to preserving the good name of the Swiss banking community, nationally and internationally,
- with a view to establishing rules ensuring, in the area of banking secrecy and when entering into business relations, business conduct that is beyond reproach,
- with an effort to provide effective assistance in the fight against money laundering and against financing acts of terrorism,

the banks hereby contract with the Swiss Bankers Association in its capacity as the professional body charged with safeguarding the interests and reputation of Swiss banking:

- a) to verify the identity of their contracting partners and, in cases of doubt, to obtain from the contracting partner a declaration setting forth the identity of the beneficial owner of assets;
- b) not to provide any active assistance in the flight of capital;
- c) not to provide any active assistance in cases of tax evasion or similar acts, by delivering incomplete or misleading attestations.

- 1 ¹ This agreement applies to the signatory banks and all their branches located in Switzerland, but not to their foreign branches, representative offices and subsidiary companies (cf., however, points 11, 19 and 21).

² The banks may, however, not misuse their foreign branches and group companies engaging in banking and finance to circumvent this agreement.

- 2 This agreement in no way modifies the obligation to observe banking confidentiality. It cannot and is not intended to
 - extend to Swiss territory the area of application of foreign legislation in economic, fiscal and currency matters, or declare such legislation to be applicable to Swiss banks (unless this is already

- provided for under current international treaties and Swiss law);
 - depart from current legal practice in the field of international law;
 - modify provisions under civil law governing relations between banks and their customers.
- 3 This agreement lays down, with binding effect, valid rules of good conduct in bank management as a code of professional ethics. They should put in concrete terms certain points of due diligence governed by the Anti Money Laundering Act (art. 3 through 5 of the AMLA) and “the diligence that can be reasonably expected under the circumstances” (art. 305^{ter} of the Swiss Penal Code)¹. Special due diligence rules for business relations and transactions involving higher risks are set forth in the Anti Money Laundering Ordinance by the Swiss Federal Banking Commission. – This is not intended to impede normal banking business.

¹ Separate regulations govern the analogous application of the CDB to the business practice of credit card companies.

A Verification of the Contracting Partner's Identity and Declaration of Identity of the Beneficial Owner

Art. 2 Verification of the contracting partner's identity

¹ The banks undertake to verify the identity of the contracting partner when establishing business relations with said partner.

² This regulation applies to:

- opening of accounts or passbooks;
- opening of securities accounts;
- entering into fiduciary transactions;
- renting of safe-deposit boxes;
- entering into management agreements for assets deposited with third parties;
- the execution of transactions with securities, currencies as well as precious metals and other commodities exceeding the amount of CHF 25,000.
- cash transactions exceeding the amount of CHF 25,000.

I. Scope of application

- 4 The obligation to verify identity is valid, subject to point 18, regardless of whether the accounts, passbooks and securities accounts of any kind whatsoever, or the safe-deposit boxes, are maintained under the name of the contracting partner or under a number (art. 9).
- 5 In the case of bearer savings books, the bank must verify the identity of any persons who deposit or withdraw amounts exceeding CHF 25,000. New bearer savings books must not be opened.
- 6 Securities are deemed to be standardized securities suitable to be traded in large quantities, non-certificated stocks of equal function (inscribed stocks) and derivatives (cf. art. 2 lit. a of the Swiss

Stock Exchange Act). This definition also subsumes non-standardized financial products.

- 7 Cash transactions refer to transactions carried out at a bank's teller window (currency exchange, purchase and sale of precious metals, cash subscriptions to bank "cash bonds" and debenture loans, cash sale of travellers checks, cashing of checks, etc.). Cash deposits into and cash withdrawals from as well as the delivery of securities into or out of existing accounts/passbooks are not deemed cash transactions (subject to point 5).

- 8 ¹The bank shall verify the identity of the contracting partner when entering into transactions below the minimum limit (art. 2, par. 2, 6 and 7 lemma) if it is obvious that the transaction has been split up with the purpose of avoiding verification of identity (so-called "smurfing").

² If the bank has cause to suspect that the assets originate from sources described in art. 9 par. 1 of the AMLA, it has to verify the identity of the contracting partner, regardless of minimum limits (art. 2, par. 2, 6 and 7 lemma) or exceptions to formal identification (point 18 of this agreement). This is not applicable if the bank declines to carry out the transaction for or to enter into a business relation with said contracting partner.

II. Verification of the contracting partner's identity

1. Individuals
 - a) In the case of personal negotiations between the party concerned and the bank
- 9 When the party concerned personally enters into negotiations with the bank, the bank verifies the identity of the contracting partner by examining and making a photocopy of an official iden-

- tification document with a photograph (passport, identity card, driving license or some similar document) and puts on record the data required in point 22.
- b) in the case of business relations entered into through correspondence
- 10 In the case of business relations entered into through correspondence or by internet, the bank verifies the identity of the contracting partner by obtaining a certified copy of an official identification document as set forth in point 9. above, as well as a confirmation of the domicile indicated, either through an exchange of correspondence or by any other appropriate method.
- 11 ¹ The authentication of the copy of the official identification document may be provided by:
- a) a branch, representative office or group company of the bank,
 - b) a correspondent bank or some other financial intermediary specifically appointed by the account opening bank,
 - c) a public notary or another public office that customarily issues such authentications.
- ² The identification based on an official identification document at delivery or receipt of mail is also deemed as sufficient proof of identity, provided that personal delivery to the recipient is thus warranted.
2. Legal entities and companies
- a) with registered office in Switzerland
- 12 The bank ascertains whether the firm's name is published in the official Swiss Commerce Gazette ("Schweizerisches Handelsamtsblatt / Feuille officielle suisse du commerce") or listed on a public website for commercial register entries (e.g. www.zefix.ch). The

bank may also use relevant private directories and databases (“Schweizerisches Rationenbuch / Annuaire suisse du Registre du commerce”). Otherwise, the identity must be established by means of an extract from the Commercial Register (“Handelsregister / Registre du commerce”).

- 13 The identity of legal entities and partnerships not listed in the Commercial Register (associations, foundations, collective condominium ownerships, independent public institutions and corporations) is verified on the basis of charters or any other equivalent document.

b) with registered office abroad

- 14 The identity of the contracting partner is verified by means of an extract from the Commercial Register or an equivalent document or extracts from public websites for Commercial Register entries or equivalent documents, substantiating the existence of the legal entity or company (such as a certificate of incorporation).

c) Common provisions

- 15 The extract from the Commercial Register or equivalent document must not be dated older than 12 months. A document dated older than 12 months may be used in conjunction with an audit report or a „certificate of good standing“ dated not older than 12 months.
- 16 The verification of identity for associations, foundations and partnerships not entered in a Commercial Register, must include the verification of identity and documents for the persons opening the account, if they are authorised signatories.
- 17 ¹ The identification requirements of a legal entity as set forth in

points 12 to 14 may be waived if the identity of the contracting partner is publicly known. The identity is deemed publicly known if it is a public company or associated directly or indirectly with a public company. The bank must keep on file a record of the justification for waiving the procedures as set forth in points 12 to 14.

² The simplified procedure as stipulated in par. 1 is not applicable to domiciliary companies unless they are associated directly or indirectly with a public company.

3. Exceptions

- 18 It is not necessary to formally verify the identity of a contracting partner when opening
 - a) an account, deposit account or passbook in the name of a minor, provided that the assets deposited with the bank at the outset do not exceed an amount of CHF 25,000; however, the identity of the account opening adult person has to be verified; point 22 applies analogously; if the person opening an account, securities account or passbook is minor, the identity of such minor person has to be verified;
 - b) a rent guaranty account for a rented property located in Switzerland;
 - c) an account with a view to paying up capital stock in connection with the formation of a corporation or a limited liability company or an increase of its capital.
- 19 The procedure as set forth in points 9 to 14 becomes redundant if the contracting partner's identity had been verified previously in an equivalent manner within the bank's group. In this case, the respective members of the bank's group must hold copies of the original identification files. This provision is not applicable in cases where such transfer of data is banned by law.

- 20 In cases where the identity of the contracting partner cannot be verified in the manner required, for instance because an individual has no identity documents or because no official documents exist for a public corporation or institution, the bank may verify the identity in another effective manner by requiring other relevant documents or by obtaining relevant credentials from public authorities or, for legal entities, by obtaining the latest statement from an authorised auditing firm. Credentials and photocopies of alternative documents have to be kept on file, as well as an internal memorandum stating the reason for the exemption.

4. General regulations of identity verification and supervision

- 21 ¹ The Bank may appoint an individual or a company by written agreement to verify the identity of a contracting partner, provided that

- a) such mandatory has been instructed accordingly by the bank, and
- b) the bank is able to monitor the proper execution of the verification of identity.

²The mandatory has to forward all identification documents to the bank and certify that any photocopies forwarded are identical with the corresponding originals.

³The appointment of a third party by the mandatory is prohibited.

- 22 Appropriate record is to be kept of the contracting partner's full name, date of birth, nationality and address of domicile (the firm's name and business address, if the contracting partner is a legal entity or a company), as well as of the means used to verify the identity. The date of birth and address of domicile may be omitted, if the contracting partner is domiciled in a country where such data is not customarily registered. A photocopy of the official document of identification and other identification documents must be kept on file.

- 23 The bank undertakes to ensure that its internal auditing department and the external auditing firm required by the Bank Act are in a position to verify that the required identification procedures have been complied with.
- 24 On principle, the complete credentials have to be in place in the appropriate form before an account can be used. If the bank is able to ensure through its control systems that any outstanding documents will be submitted within 30 days, an exception may be made to the effect of activating the account prior to the receipt of such documents. In this case, however, no withdrawals may be made by the client. If the documents remain outstanding after 30 days, the account has to be blocked. The bank has to terminate the business relationship if the documents are not complete within 90 days (cf. also art. 6, par. 4).

Art. 3 Establishing the identity of the beneficial owner

¹ All due diligence which can be reasonably expected under the circumstances must be exercised in establishing the identity of the beneficial owner. If there is any doubt as to whether the contracting partner is himself the beneficial owner, the bank shall require by means of Form A a written declaration setting forth the identity of the beneficial owner.

² This regulation applies to:

- opening of accounts or passbooks;
- opening of securities accounts;
- entering into fiduciary transactions;
- entering into management agreements for assets deposited with third parties;
- the execution of transactions with securities, currencies as well as precious metals and other commodities exceeding the amount of CHF 25,000.

³ If the amount of a cash transaction as per art. 2 exceeds

CHF 25,000, the bank must require the contracting partner to provide a declaration setting forth the identity of the beneficial owner. The bank shall keep such declaration on record in an appropriate manner. The use of Form A is optional.

- 25 ¹ The bank may assume that the contracting partner is also the beneficial owner, but such an assumption is invalid if unusual observations are made.

²The following cases would give rise to doubt:

- when a power of attorney is conferred on someone who evidently does not have sufficiently close links to the contracting partner; this provision does not include a power of attorney for the management of asset given to a financial intermediary;
- when the financial standing of someone wishing to carry out one of the transactions described in art. 3 is known to the bank, and the assets submitted or about to be submitted are disproportionate to said person's financial standing;
- when, in the course of its relations with the customer, the bank is led to make other unusual observations.

- 26 A declaration on Form A must invariably be provided by individuals entering into a business relation with a bank through correspondence. Exempt are instances as provided in point 18.

- 27 If the contracting partner states that the beneficial owner is a third party, he or she shall fill in Form A disclosing the full name, date of birth, nationality, address and country of domicile (or the firm's name and business address, if the party is a legal entity or a company) of said third party. The bank reserves the right to apply art. 3, par. 3. The date of birth and address of domicile may be omitted, if the beneficial owner is domiciled in a country where such data is not customarily registered.

- 28 Form A may be signed by the contracting partner or his designated signatory authorised by means of a specific or general proxy. In the case of legal entities, form A or the proxy has to be signed by the registered signatories listed in the company's credentials.
- 29 If serious doubts persist about the accuracy of the contracting partner's written declaration and cannot be dispelled through further clarification, the bank shall refuse to enter into a business relationship or to execute the transaction.
- 30 Form A is attached to this agreement. This form can be obtained in English, French, German, Italian and Spanish from the office of the Swiss Bankers Association.
- 31 The banks have the right to print their own forms, reflecting their own particular requirements. These forms must contain the complete text of the sample form.
- 32 The holder of a joint account or a joint securities account is required to provide the bank with a full list of beneficial owners, pursuant to point 27, and to inform the bank of any changes without delay.
- 33 In the case of collective investments and investment companies with more than 20 investors as beneficial owners, the data as set forth in point 27 must be recorded only for the beneficial owners who hold severally or in joint agreement a minimum of 5% of the assets deposited with the bank. If the number of beneficial owners is up to 20, the bank must record the data as set forth in point 27 for all. No disclosure of beneficial owners is required in the case of collective investments listed on a stock exchange.
- 34 ¹ In principle no declaration of beneficial ownership is required for

banks domiciled in Switzerland or abroad. Their definition is governed by the relevant specific laws of their country of domicile. Beneficial ownership has to be declared for sub-accounts held on behalf of undisclosed clients by banks which are not subject to appropriate supervision and regulation in terms of anti money laundering provisions.

² No declaration of beneficial ownership is required for other financial intermediaries domiciled or resident in Switzerland. This regulation also applies to other financial intermediaries domiciled abroad, provided they are subject to adequate supervision and an adequate set of anti-money laundering regulations.

³ Other domestic and foreign financial intermediaries are deemed: fund managements, life insurance companies, brokers and tax exempt pension funds pursuant to art. 2 par. 2 of the AMLA. The definition of foreign financial intermediaries is governed by the relevant specific laws of their country of domicile.

⁴ The bank must require banks or other financial intermediaries to submit a declaration of the beneficial owners or take other measures if it has cause to assume misuse or if a general warning is issued by the Federal Banking Commission or the Swiss Bankers Association with respect to individual institutions or the institutions of a specific domicile.

- 35 ¹The establishment of the beneficial owner's identity may be delegated to a third party. The provisions under point 21 have to be applied analogously.

² Point 24 is applicable analogously in establishing the beneficial owner's identity.

- 36 The bank undertakes to ensure that the internal auditing department and the external auditing firm required by the Bank Act are in a position to verify that the identity of the beneficial owner has been established.

- 37 Special provisions apply to domiciliary companies or persons bound by professional confidentiality (art. 4 and 5, points 38 through 46).

Art. 4 Procedure for domiciliary companies

¹ Under the terms of this agreement, the entities considered domiciliary companies are institutions, corporations, foundations, trusts, etc., that do not conduct any commercial or manufacturing business or any other form of commercial operation in the country where their registered office is located.

² The banks must require that Swiss and foreign domiciliary companies provide the following documents:

- a) an extract from the Commercial Register or an equivalent credential (cf. points 12 through 16) to verify their identity;
- b) the declaration on Form A by the contracting partner indicating the beneficial owner(s) of the assets concerned.

³ The use of Form A may be waived if the bank is familiar with the beneficial owner and is in possession of the data as per point 27. The bank shall, however, keep a record of the relevant data on file.

I. Domiciliary companies

- 38 Swiss and foreign enterprises are considered domiciliary companies, regardless of their objects, function, legal form or registered office, provided:
- a) they do not have their own premises (domiciled c/o an attorney, a trust company, a bank, etc.), or
 - b) they do not have their own staff working exclusively for them, or their own staff engages solely in administrative tasks (bookkeeping and correspondence under instructions issued by individuals or companies controlling the domiciliary company).

- 39 Family foundations or other legal entities and companies whose purpose is to safeguard the interests of their members in joint self-help or who pursue primarily political, religious, scientific, artistic, welfare, social or such comparable purposes are deemed domiciliary companies if the bank concludes that the statutory purposes of such legal entities or companies are not exclusively pursued.

II. Beneficial ownership of domiciliary companies

- 40 The beneficial owner of a domiciliary company may be either an individual or a legal entity conducting a commercial or manufacturing business or any other form of commercial operation. A domiciliary company as such cannot be deemed a beneficial owner.
- 41 The identity of the beneficial owners must be established and kept on file in accordance with points 27 and 28. Point 29 refers.
- 42 The beneficial owners of a domiciliary company listed on a stock exchange need not be established.
- 43 In the case of organised associations of individuals, assets or patrimony without specific beneficial owners (eg. discretionary trusts), instead of identifying the beneficial owners on Form A the contracting partner is required to provide a written declaration confirming this fact. Such declaration must also contain information about the actual (not fiduciary) settlor and, if determinable, persons authorised to instruct the contracting partner or his or her agents, as well as persons who are likely to become beneficiaries (in categories, eg. "members of the settlor's family"). Any curators, protectors, etc. must also be included in said declaration.
- 44 In the case of revocable structures (e.g. revocable trusts), the actual settlor must be listed as beneficial owner.

III. Change in signing authority

- 45 If any changes are made in the signatures authorised by the domiciliary company in its relations with the bank, the bank must repeat the procedure set forth in art. 4, par. 2, letter b), unless the bank has evidence or is advised in writing by the management of the domiciliary company or its authorised signatories that the beneficial owners have remained unchanged. If the bank is unable to precisely establish the identity of the beneficial owners, art. 6, par. 3 is applicable.

Art. 5 Persons bound by professional confidentiality

The banks may waive the identification of beneficial owners of accounts or securities accounts held by attorneys or notaries for the account of their clients, provided that such attorney or notary is admitted to the Bar in Switzerland and declares in writing that said account or securities account is held exclusively for a purpose as stated below, and that such account or securities account is termed accordingly (type of mandate):

- a) – winding-up and, so far as appropriate, related short-term deposit of advances on legal costs, security, fees under public law, etc. as well as of payments to or from parties, third party/parties or authorities (termed “winding-up account/securities account of client’s funds”);
- b) – deposit and, so far as appropriate, related placement of assets from a pending partition of inheritance or execution of a will (termed e.g. “inheritance” or “partition of inheritance”);
 - deposit/placement of assets from a pending separation of property in the divorce or separation of a marriage (termed e.g. “separation of property/divorce of marriage”);
 - depositing of a security/placement of assets in matters of civil or public law (termed e.g. “escrow account/deposit”, “blocked deposit account for purchase of stocks”, “deposit of

a security/corporate security", "deposit of a security/property income tax", etc.);

- deposit and, so far as appropriate, related placement of assets in matters of civil and public law before ordinary courts or courts of arbitration and in execution proceedings (termed e.g. "advances", "guarantee for court security", "bankrupt's estate", "arbitration proceedings", etc.).

46 ¹ Form R is provided for the declaration under art. 5. This form can be obtained in German, French and Italian from the office of the Swiss Bankers Association in Basle.

² The banks have the right to print their own forms reflecting their own specific requirements. These forms must contain the complete text of the sample form (cf. annex).

Art. 6 Changes and errors with respect to the verification of the contracting partner's identity or the declaration of identity of the beneficial owner (art. 2 through 5 CDB)

¹ The bank has to repeat the procedure pursuant to art. 2, points 9 through 24, and art. 3 and 4, points 25 through 45

- if, during the business relationship, the bank has cause to doubt
 - the accuracy of the information about the identity of the contracting partner,
 - that the contracting partner is identical with the beneficial owner, or
 - the accuracy of the declaration of beneficial ownership,
- if there are any signs of unreported changes.

² If a bank discovers that a declaration pursuant to art. 5 of this agreement is inaccurate, it must require its contracting partner to declare the identity of the beneficial owner in Form A. If the contracting partner fails to provide a declaration setting forth the identity of the beneficial owner, the bank shall sever its business relations with said contracting partner.

³ Banks are required to sever their relations with the contracting partner if the transactions carried out give rise to the assumption that the bank has been deceived when verifying the identity of the contracting partner, that the bank was wilfully given false information about the beneficial owner or if doubts persist with regard to the contracting partner's declaration upon implementation of the procedure as required under par. 1.

⁴ Business relations must not be severed if circumstances necessitate a declaration pursuant to art. 9 of the AMLA.

- 47 Relations must be severed as quickly as it is possible to do so without violating the contract. If the bank is unable to reach the contracting partner owing to mailing instructions, it can postpone the severance of relations until the contracting partner's next visit or the bank's forwarding of correspondence.

B Prohibition against active Assistance in the Flight of Capital

Art. 7 Flight of capital

Banks may not provide any active assistance whatsoever in transferring capital outside countries whose laws prohibit said transfers or impose restrictions on the placing of funds abroad.

48 ¹ Flight of capital is an unauthorised transfer of capital in the form of foreign exchange, banknotes or securities from a country that forbids or restricts such transfer abroad by its residents.

² The mere duty to report cross-border currency transfers is not deemed a restriction of capital movement.

49 Art. 7 does not apply to the transfer abroad of capital from Switzerland.

50 The following acts constitute active assistance:

- a) receiving clients abroad by appointment outside the bank's own premises, for the purpose of accepting funds;
- b) participation abroad in the setting up of offset transactions when the bank knows or, based on a combination of circumstances, should know that the offset is aimed at furthering the flight of capital;
- c) active collaboration with individuals and companies that arrange for the flight of capital on behalf of third parties or who provide assistance to this effect:
 - by remitting orders;
 - by promising them commissions;
 - by keeping their accounts, while the bank is aware that such individuals or companies are using their accounts for business purposes to assist in the flight of capital;

- d) referring customers to the persons and companies described in letter c).
- 51 Visits to customers abroad are permitted provided the officer acting on behalf of the bank does not accept any funds that may not be legally transferred, gives no advice to assist in the illegal transfer of capital and does not participate in any offset transactions.
- 52 Otherwise, assets for foreign customers may be accepted in Switzerland.

C Prohibition against active Assistance in Tax Evasion and Similar Acts

Art. 8 Tax evasion and similar acts

Banks shall not provide any assistance to their customers in acts aimed at deceiving Swiss and foreign authorities, particularly tax authorities, by means of incomplete or otherwise misleading attestations.

- 53 ¹ It is forbidden to remit to the customer personally or, at his or her request, directly to Swiss or foreign authorities, any incomplete or otherwise misleading attestations.

² Authorities include, in particular, tax, customs, currency and bank supervisory authorities as well as prosecution authorities.

- 54 ¹ Subject to this prohibition are special attestations requested by the customer for submission to authorities.

² The bank is not permitted to alter routine records, such as statements of account and securities, credit and debit advices, settlement notes for foreign exchange transactions, coupon and stock exchange transactions, for the purpose of deception.

- 55 ¹ Attestations are incomplete if significant facts are omitted in order to deceive authorities; for example if the bank, at the given request of the customer, omits certain items from a given attestation or from a statement of account or securities.

² It is not necessary to mention in the statements of account or deposit that the same customer holds other accounts or deposits.

- 56 Attestations are misleading if the facts are presented in an untruthful manner to deceive the authorities, such as:

a) by showing false dates, false amounts or fictitious rates or by issuing credit and debit advices showing false information about the persons debited or credited;

- b) by attesting to fictitious claims or debts (regardless of whether or not the attestation reflects the bank's records).
- c) by allowing customers to use the bank's nostro accounts for the purpose of cutting tax duties.

D Other Provisions

Art. 9 Numbered accounts

The provisions of this agreement apply without restriction to accounts, passbooks, securities accounts and safe deposits designated by a number or code.

- 57 Numbered or coded accounts, securities accounts, including fiduciary deposits, must be included in the attestations covering all the business relations with the customer.

Art. 10 Auditing

¹ By signing this agreement, the banks instruct and authorise their external bank auditors under the Bank Act to ascertain through random tests conducted during the regular auditing of the accounts that the provisions of this agreement have been complied with. The auditors required under the Bank Act shall inform the Supervisory Board set up pursuant to art. 12 and the Federal Banking Commission of any violations they may uncover or have reason to suspect.

² All officially recognised external bank auditors in Switzerland shall receive a copy of this agreement, together with a list of signatories, from the Swiss Bankers Association. This constitutes their auditing mandate.

Art. 11 Violation of the agreement; sanctions

¹ In the event this agreement is violated, the culpable bank is required to pay the Swiss Bankers Association a fine of up to 10 million Swiss francs. In fixing this fine, due account is taken of the seriousness of the violation, of the degree of culpability and of the bank's financial situation. Measures imposed by other authorities with respect to the same issue are to be taken into account. The amount of the fine is determined in accordance with the procedure

provided under art. 12 and, if appropriate, art. 13. The Swiss Bankers Association may use the fine to cover any negative cost balance and allocates the remaining amount of the fine to a useful public purpose at its own discretion.

² In minor cases, the culpable bank may be sent a note of reprimand instead of being required to pay a fine.

³ A fine or reprimand will only be decreed in the case of a violation of art. 6 par. 1 and 2 as a result of gross negligence, or in the case of intentional violations of art. 7 and 8.

⁴ The prosecution of a violation of this agreement is barred by statute upon a lapse of 5 years. In the case of a violation of the duty to verify the identity of the contracting partner and to establish the identity of the beneficial owner, the five-year statute period starts as of the rectification of the violation or the severance of the business relation.

Art. 12 Supervisory Board, Investigators

¹ The Swiss Bankers Association sets up a Supervisory Board composed of five independent experts, with a view to investigating and penalising violations under this agreement. The Supervisory Board appoints a secretary and regulates his or her responsibilities.

² The Swiss Bankers Association appoints one or more investigators. The investigators may recommend to the Supervisory Board that proceedings be opened and sanctions imposed or that the investigation be terminated. When requesting information from a bank, the investigators have to inform the bank of the capacity in which it is involved in the proceeding.

³ The members of the Supervisory Board and the investigators are appointed for a term of five years, and may be reappointed.

⁴ If the Supervisory Board finds that the agreement has been violated, it imposes an equitable sanction upon the culpable bank, in accordance with art. 11 above.

⁵ The Supervisory Board establishes the rules of procedure and determines the allocation of costs.

⁶ If the culpable bank abides by the decision of the Supervisory Board, the proceeding is closed. Otherwise, art. 13 applies.

⁷ If a bank refuses to participate in the investigation conducted by the Supervisory Board or by the investigators, the Supervisory Board may impose a fine pursuant to art. 11.

⁸ As authorised officers under the terms of art. 47 of the Bank Act, the members of the Supervisory Board, the secretary and the investigators are strictly bound to treat as confidential the facts about which they gain knowledge in the course of the proceeding. The banks may not invoke banking confidentiality vis-à-vis the Supervisory Board or the investigators.

⁹ The Supervisory Board informs the Federal Banking Commission of its decisions. If it determines that abuses have been committed by persons subject to professional confidentiality, the Supervisory Board may also advise the appropriate disciplinary authority thereof.

- 58 The Supervisory Board periodically informs the banks and the general public of its findings, to the extent permitted by the rules of banking and business confidentiality.
- 59 The Supervisory Board may – in agreement with the Board of Directors of the Swiss Bankers Association – provide the banks with interpretations of this agreement. Banks shall submit according applications to the Swiss Bankers Association.

Art. 13 Arbitration procedure

¹ If the fine set by the Supervisory Board has not been paid by the date prescribed, an arbitration tribunal based in Basle will hand down, upon a complaint brought by the Swiss Bankers Association

against the bank concerned, a final decision as to whether there has or has not been a violation of the terms of this agreement and, if applicable, will decide on the fine to be imposed. To this effect the banks submit themselves to the jurisdiction of the courts of Basle.

² The Swiss Bankers Association and the bank each appoint an arbitrator and the two arbitrators thus appointed jointly nominate an umpire.

³ A petition for arbitration becomes pending as soon as the Swiss Bankers Association has designated the arbitrator it is entitled to appoint.

⁴ If a party has not appointed its arbitrator within 30 days from receipt of the written notification from the other party announcing that arbitration proceedings have been commenced, or if the two arbitrators have not been able to agree on the appointment of an umpire within 30 days following acceptance of their appointment as arbitrators, the Court of Appeals ("Appellationsgericht") of the Canton of the City of Basle will proceed, at the request of one of the parties, to make the appointment.

⁵ If an arbitrator is unable to discharge his office for any reason whatsoever, the party who appointed him must appoint a new arbitrator within 30 days, failing which the Court of Appeals of the City of Basle will proceed, at the request of the other party, to nominate the arbitrator.

⁶ If the umpire is unable to discharge his office for any reason whatsoever, the two arbitrators must again name an umpire. If they fail to reach an agreement, the Court of Appeals of the Canton of the City of Basle will proceed with the appointment, at the request of either of the parties.

⁷ If an arbitrator or an umpire is replaced in accordance with par. 5 and 6 above, the records of the proceedings in which the latter participated remain valid.

⁸ Subject to the mandatory provisions of the Swiss Concordat on Arbitration and of the Code of Civil Procedure of the Canton of the City of Basle, the provisions of the latter apply only if the parties or, failing them, the court of arbitration adopt no other rule of procedure. The maxim of contingency is applicable no earlier than as of the second exchange of pleadings.

⁹ The court of arbitration is subject to the same rule of confidentiality as that set forth in art. 12, par. 8.

Art. 14 Entry into force

¹ This agreement takes effect on 1st July 2003.

² The Swiss Bankers Association and each signatory bank may withdraw from this agreement, subject to three months notice, with withdrawal taking effect at the end of a contractual year but not earlier than 30th June 2008.

³ The Swiss Bankers Association reserves the right to apprise the banks of supplementary regulations during the life of the agreement, upon agreement with or request by the Federal Banking Commission (cf. art. 16 AMLA).

⁴ The Swiss Bankers Association reserves the right to unilaterally adjust or cancel the sanction rules (art. 11 through 13), if amended legal provisions or new legal practice should lead to inappropriate multiple sanctions for the same facts.

Art. 15 Transitional regulation

¹ The revised Form A is to be applied, if, upon entry into force of this agreement, a new business relationship is entered into or if the procedure of establishing the identity of a beneficial owner is to be repeated pursuant to art. 6 of this agreement.

² The new regulations governing the verification of identity of contracting partners and declaration of identity of the beneficial owners are applicable to new business relations entered into upon

the date of enactment of this agreement or if the establishing of beneficial ownership must be revised pursuant to art. 6 upon the date of enactment of this agreement. The new agreement may be applied to existing business relations if it is deemed more beneficial.

A

Account No.:

Contracting partner:

Establishment of the Beneficial Owner's Identity

(Form A as per art. 3 and 4 CDB)

The contracting partner hereby declares:

(mark with a cross where appropriate)

☐ that the contracting partner is the sole beneficial owner of the assets concerned☐ that the beneficial owner/s of the assets concerned is/are:

Full name (or Company), Date of Birth, Nationality, Address/Domicile, Country

The contracting partner undertakes to inform the bank, of his own accord, about any changes.

Willfully entering false information in this form is a criminal offense (art. 251 of the Swiss Penal Code, forgery of documents; under penalty of up to five years of hard labor or prison).

Place and date

Signature of the contracting partner

351

EBK Bulletin 44/2003

R

Account No. :

Contracting Partner:

Term:

**Declaration by Swiss attorney or notary
Upon opening an account or securities account**

The undersigned hereby declares that he/she acts as attorney/notary* and that he/she is subject to corresponding provisions by cantonal laws.

He/she declares that he/she is not entitled to beneficial ownership of the assets deposited with the bank. He/she certifies that, with regard to the aforesaid account/securities account, he/she is subject to **professional confidentiality as protected by art. 321 SPC (Swiss Penal Code) and that said account/securities account serves the sole purpose of:**

☐ winding-up and, so far as appropriate, related short-term deposit of advances on legal costs, security, fees under public law, etc. as well as of payments to or from parties, third party/parties or authorities (termed "winding-up account/securities account of client funds");

☐ deposit and, so far as appropriate, related placement of assets from a pending partition of inheritance or execution of a will (termed e.g. "inheritance" or "partition of inheritance");

deposit and, so far as appropriate, placement of assets from a pending separation of property in the divorce or separation of marriage (termed e.g. "separation of marital property/divorce");

depositing of a security and, so far as appropriate, placement of assets in matters of civil or public law (termed e.g. "escrow account/deposit", "blocked deposit account for purchase of stocks", "deposit of a security/corporate security", "deposit of a security/property income tax" etc.);

deposit and, so far as appropriate, related placement of assets in matters of civil and public law before ordinary courts or courts of arbitration and in execution proceedings (termed e.g. "advances", "guarantee for court security", bankrupt's estate", "arbitration proceedings" etc.)

(Mark with a cross where applicable; only **one** square is to be marked.)

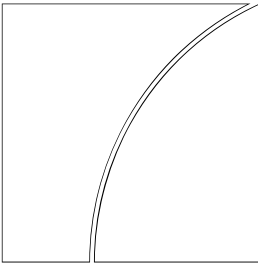
Place and date

Signature

*delete where inapplicable

Willfully entering false information in this form is a criminal offence (art. 251 of the Swiss Penal Code, forgery of documents; under penalty of up to five years of hard labor or prison).

Basler Ausschuss
für Bankenaufsicht



Sorgfaltspflicht der Banken bei der Feststellung der Kundenidentität

Oktober 2001

353

EBK Bulletin 44/2003



BANK FÜR INTERNATIONALEN ZAHLUNGS AUSGLEICH

Arbeitsgruppe für das grenzüberschreitende Bankgeschäft

Vorsitzende:

Charles Freeland, Stellvertretender Generalsekretär, Basler Ausschuss für Bankenaufsicht

Colin Powell, Vorsitzender, Offshore-Gruppe von Bankenaufsichtsbehörden, und Vorsitzender, Jersey Financial Services Commission

Bermuda Monetary Authority

Cayman Islands Monetary Authority

Banque de France/Commission Bancaire

Bundesaufsichtsamt für das Kreditwesen

Guernsey Financial Services Commission

Banca d'Italia

Financial Services Agency, Japan

Commission de Surveillance du Secteur Financier,
Luxemburg

Monetary Authority of Singapore

Eidgenössische Bankenkommision

Financial Services Authority, Vereinigtes Königreich

Board of Governors of the Federal Reserve System

Federal Reserve Bank of New York

Office of the Comptroller of the Currency

Sekretariat

Herr D. Munro Sutherland

Herr John Bourbon
Frau Anna McLean

Herr Laurent Ettori

Herr Jochen Sanio
Herr Peter Kruschel

Herr Peter G. Crook (bis April 2001)
Herr Philip Marr (seit April 2001)

Herr Giuseppe Godano

Herr Kiyotaka Sasaki (bis Juli 2001)
Herr Hisashi Ono (seit Juli 2001)

Herr Romain Strock

Frau Foo-Yap Siew Hong
Frau Teo Lay Har

Herr Daniel Zuberbühler
Frau Dina Balleyguier

Herr Richard Chalmers

Herr William Ryback

Frau Nancy Bercovici

Herr Jose Tuya
Frau Tanya Smith

Herr Andrew Khoo

Inhaltsverzeichnis

I.	Einleitung	1
II.	Bedeutung von Standards zur Feststellung der Kundenidentität für Aufsichtsbehörden und Banken	2
III.	Wesentliche Elemente der Standards für die Feststellung der Kundenidentität	4
1.	Regelungen für die Annahme von Kunden	4
2.	Identifizierung der Kunden	5
2.1	Allgemeine Anforderungen der Kundenidentifizierung	6
2.2	Besondere Identifikationsprobleme	6
2.2.1	Trust-, Treuhand- und ähnliche Konten	6
2.2.2	Juristische Personen	7
2.2.3	Eingeführte Kunden	7
2.2.4	Von professionellen Vermittlern eröffnete Kundenkonten	8
2.2.5	Politisch exponierte Personen	8
2.2.6	Kunden, die nicht persönlich vorsprechen	9
2.2.7	Korrespondenzbankensystem	10
3.	Fortlaufende Überwachung von Konten und Transaktionen	11
4.	Risikomanagement	11
IV.	Rolle der Aufsichtsbehörden	12
V.	Umsetzung von Standards für die Feststellung der Kundenidentität im grenzüberschreitenden Geschäft	13
	Anhang 1: Auszug aus der <i>Methodik der Grundsätze für eine wirksame Bankenaufsicht</i>	15
	Anhang 2: Auszug aus den Empfehlungen der FATF	17

Sorgfaltspflicht der Banken bei der Feststellung der Kundenidentität

I. Einleitung

1. Aufsichtsinstanzen in aller Welt erkennen immer mehr, wie wichtig es ist, dafür zu sorgen, dass die ihnen unterstellten Banken über angemessene Kontrollen und Verfahren verfügen, damit sie ihre Vertragspartner kennen. Eine angemessene Sorgfalt hinsichtlich neuer und bisheriger Kunden ist ein Schlüsselement dieser Kontrollen. Ohne diese Sorgfalt können Banken operationellen, Rechts-, Reputations- und Konzentrationsrisiken ausgesetzt sein, die erhebliche finanzielle Kosten zur Folge haben können.

2. Anhand der Ergebnisse einer 1999 durchgeführten internen Erhebung über das grenzüberschreitende Bankgeschäft hat der Basler Ausschuss festgestellt, dass die Vorschriften für die Feststellung der Kundenidentität durch die Banken in vielen Ländern mangelhaft sind. Aus der Aufsichtsperspektive bestehen in manchen Ländern erhebliche Lücken, in anderen gibt es in diesem Bereich überhaupt keine Vorschriften. Selbst bei Ländern mit gut ausgebauten Finanzmärkten sind die Vorschriften unterschiedlich solide. Daher hat der Basler Ausschuss die Arbeitsgruppe für das grenzüberschreitende Bankgeschäft¹ gebeten, die aktuellen Verfahren für die Feststellung der Kundenidentität zu prüfen und Empfehlungen für Standards zu erarbeiten, die für die Banken in allen Ländern gelten sollen. Das Ergebnis wurde im Januar 2001 als Konsultationspapier veröffentlicht. Nach Prüfung der eingegangenen Stellungnahmen hat die Arbeitsgruppe das Papier überarbeitet, und der Basler Ausschuss verbreitet es jetzt auf weltweiter Basis. Der Ausschuss geht davon aus, dass die hier vorgestellte Rahmenregelung zum Massstab wird, anhand dessen die Aufsichtsbehörden nationale Vorschriften für die Feststellung der Kundenidentität erlassen und die Banken ihre eigenen Systeme gestalten. Freilich ist das Ziel des vorliegenden Papiers in einigen Rechtsordnungen bereits erreicht oder wird sogar überschritten, so dass dort möglicherweise keine Änderungen notwendig sind.

3. Die Feststellung der Kundenidentität steht in engem Zusammenhang mit der Bekämpfung der Geldwäsche, die im wesentlichen in den Aufgabenbereich der Financial Action Task Force (FATF) fällt.² Der Ausschuss will die Arbeit der FATF nicht duplizieren. Vielmehr befasst er sich mit dem Thema aus einer erweiterten aufsichtlichen Perspektive. Solide Vorschriften und Verfahren zur Feststellung der Kundenidentität sind entscheidend, um die Sicherheit und Solidität der Banken und die Integrität des Bankensystems zu wahren. Der Basler Ausschuss und die Offshore-Gruppe von Bankenaufsichtsbehörden (Offshore Group of Banking Supervisors, OGBS) unterstützen weiterhin nachdrücklich die Übernahme und Umsetzung der FATF-Empfehlungen, insbesondere soweit sie sich auf die Banken beziehen; die hier vorgelegten Standards sollen mit den FATF-Empfehlungen vereinbar sein. Sollte die FATF nach ihrer derzeitigen Überprüfung der 40 Empfehlungen strengere Standards einführen, werden der Ausschuss und die OGBS deren Verabschiedung ebenfalls prüfen. Die Arbeitsgruppe pflegt daher engen Kontakt mit der FATF und verfolgt deren Überlegungen.

4. Der Basler Ausschuss befasst sich mit der Feststellung der Kundenidentität nicht nur im Hinblick auf die Bekämpfung der Geldwäsche, sondern aus einer erweiterten aufsichtlichen Perspektive. Solide Verfahren für die Feststellung der Kundenidentität sind als entscheidende Voraussetzung für ein wirksames Risikomanagement im Bankgeschäft zu sehen. Die Schutzmechanismen gehen über einfache Kontoeröffnungen und das Aufbewahren von Unterlagen hinaus; sie verlangen von den Banken die Formulierung von Regelungen für die Annahme von Kunden sowie ein gestaffeltes System für die Feststellung der Kundenidentität. Dieses System beinhaltet eine umfassendere

¹ Eine Gruppe, in der Mitglieder des Basler Ausschusses für Bankenaufsicht und der Offshore-Gruppe von Bankenaufsichtsbehörden vertreten sind.

² Die FATF ist ein zwischenstaatliches Gremium, das auf nationaler und internationaler Ebene Massnahmen zur Bekämpfung der Geldwäsche entwickelt und fördert. Es hat 29 Mitgliedsländer und zwei regionale Organisationen. Es arbeitet eng mit anderen in diesem Bereich tätigen internationalen Gremien zusammen, z.B. dem Büro der Vereinten Nationen für Drogenkontrolle und Verbrechensverhütung, dem Europarat, der Asia-Pacific Group on Money Laundering und der Caribbean Financial Action Task Force. Die FATF definiert Geldwäsche als die Verarbeitung von Erträgen aus verbrecherischen Geschäften mit dem Ziel, ihren illegalen Ursprung zu verschleiern.

Sorgfaltspflicht für Geschäftsverbindungen mit höherem Risiko sowie eine aktive Überwachung der Geschäftsverbindungen auf verdächtige Vorgänge.

5. Das Interesse des Basler Ausschusses an soliden Standards für die Feststellung der Kundenidentität entstammt seinem Bemühen um die Marktintegrität und wurde verstärkt durch die direkten und indirekten Verluste, die Banken aufgrund mangelnder Sorgfalt bei der Anwendung geeigneter Verfahren erlitten. Diese Verluste hätten wahrscheinlich vermieden werden können und das Ansehen der Banken hätte erheblich weniger gelitten, wenn die Banken wirksame Systeme für die Feststellung der Kundenidentität gehabt hätten.

6. Das vorliegende Papier stärkt die in früheren Ausschusspapieren aufgestellten Grundsätze, indem es genauer auf die wesentlichen Elemente der Standards für die Feststellung der Kundenidentität und ihre Umsetzung eingeht. Dabei hat sich die Arbeitsgruppe auf die Praxis in den Mitgliedsländern gestützt und die Entwicklung im Aufsichtsbereich berücksichtigt. Die hier vorgestellten wesentlichen Elemente können als Grundlage für Mindeststandards zur weltweiten Einführung für alle Banken dienen. Diese Standards müssen eventuell durch zusätzliche Massnahmen, die auf die Risiken bestimmter Institute sowie Risiken im Bankensystem einzelner Länder zugeschnitten sind, ergänzt und/oder gestärkt werden. Eine grössere Sorgfalt ist z.B. notwendig bei risikoreichen Konten oder bei Banken, die speziell für Kunden mit hohem Nettovermögen attraktiv sein wollen. In etlichen Abschnitten des vorliegenden Papiers werden gegebenenfalls höhere Sorgfaltsstandards für stärker risikobehaftete Bereiche einer Bank empfohlen.

7. Nicht nur Banken müssen hinsichtlich der Sorgfalt bei der Feststellung der Kundenidentität strengen Standards genügen. Der Basler Ausschuss ist der Ansicht, dass ähnliche Richtlinien auch für alle Nichtbankfinanzinstitute sowie für professionelle Vermittler von Finanzdienstleistungen wie Rechtsanwälte und Treuhänder entwickelt werden müssen.

II. Bedeutung von Standards zur Feststellung der Kundenidentität für Aufsichtsbehörden und Banken

8. Die FATF und andere internationale Gremien haben sich intensiv mit Fragen der Feststellung der Kundenidentität beschäftigt, und die 40 Empfehlungen der FATF zur Bekämpfung der Geldwäsche³ werden international anerkannt und angewandt. Mit dem vorliegenden Papier soll diese Arbeit nicht dupliziert werden.

9. Gleichzeitig sind solide Verfahren zur Feststellung der Kundenidentität für die Sicherheit und Solidität von Banken besonders relevant, denn:

- Sie tragen dazu bei, das Ansehen der Banken und die Integrität der Bankensysteme zu schützen, indem sie die Wahrscheinlichkeit reduzieren, dass die Banken ein Werkzeug oder ein Opfer von Finanzkriminalität werden, was ihren Ruf entsprechend beeinträchtigen würde.
- Sie bilden einen wesentlichen Bestandteil eines soliden Risikomanagements (z.B. indem sie die Basis für die Ermittlung, Begrenzung und Kontrolle der Risikopositionen bei Aktiva und Passiva, einschliesslich bei für Dritte verwalteten Vermögenswerten, liefern).

10. Wenn die Standards für die Feststellung der Kundenidentität unzureichend sind oder ganz fehlen, können den Banken schwerwiegende Kunden- und Adressenausfallrisiken entstehen, insbesondere **Reputationsrisiken, operationelle Risiken, Rechts- und Konzentrationsrisiken**. Es ist festzuhalten, dass diese Risiken alle miteinander im Zusammenhang stehen. Jedes einzelne von ihnen kann den Banken jedoch erhebliche finanzielle Kosten verursachen (z.B. durch den Abzug von Einlagen, die Aufhebung von Interbank-Kreditlinien, Forderungen gegen die Bank, Untersuchungskosten, die Beschlagnahmung oder Sperrung von Aktiva sowie Kreditausfälle) und dazu führen, dass die Geschäftsleitung viel Zeit und Mühe aufwenden muss, um auftretende Probleme zu lösen.

³ S. die in Anhang 2 wiedergegebenen FATF-Empfehlungen 10-19.

11. Das **Reputationsrisiko** stellt für Banken eine grosse Bedrohung dar, da die Natur ihres Geschäfts verlangt, dass sie sich das Vertrauen ihrer Einleger und Gläubiger sowie des Marktes generell erhalten. Das Reputationsrisiko wird definiert als die Gefahr, dass negative Publizität über das Geschäftsgebahren und die Geschäftsverbindungen einer Bank, ob zutreffend oder nicht, das Vertrauen in die Integrität des Instituts beeinträchtigt. Die Banken sind gegenüber dem Reputationsrisiko besonders anfällig, da sie sehr leicht von ihren Kunden als Vehikel für deren illegale Tätigkeit benutzt oder deren Opfer werden können. Sie müssen sich daher durch ständige Wachsamkeit und ein wirksames System der Kundenidentifizierung schützen. Verwaltete oder treuhänderisch gehaltene Vermögenswerte können mit einem besonders grossen Reputationsrisiko behaftet sein.

12. Das **operationelle Risiko** lässt sich definieren als die Gefahr von unmittelbaren oder mittelbaren Verlusten, die infolge der Unangemessenheit oder des Versagens von internen Verfahren, Menschen und Systemen oder wegen externer Ereignisse eintreten. Im Zusammenhang mit der Kundenidentifizierung tritt das operationelle Risiko meist in Form von Schwächen bei der Umsetzung der Programme der Bank, unwirksamen Kontrollverfahren und mangelnder Sorgfalt auf. Gewinnt die Öffentlichkeit den Eindruck, dass eine Bank ihr operationelles Risiko nicht im Griff hat, kann sich dies sehr negativ auf die Geschäfte der Bank auswirken.

13. Das **Rechtsrisiko** ist die Möglichkeit, dass Prozesse, Gerichtsurteile gegen die Bank oder Verträge, die sich als undurchsetzbar erweisen, die Geschäfte oder die Verfassung der Bank beeinträchtigen. Gegen eine Bank kann ein Gerichtsverfahren eingeleitet werden, wenn sie zwingende Vorschriften über die Feststellung der Kundenidentität oder ihre Sorgfaltspflicht nicht einhält. Einer Bank kann dann beispielsweise eine Geldbusse auferlegt werden, sie kann strafrechtlich haftbar gemacht werden, oder die Aufsichtsbehörde kann besondere Sanktionen gegen sie verhängen. Die Kosten, die einer Bank aus einem Gerichtsverfahren gegen sie erwachsen, können zudem weit über die Verfahrenskosten hinausgehen. Eine Bank kann sich nur dann wirksam gegen solche Rechtsrisiken schützen, wenn sie bei der Identifizierung ihrer Kunden und der Kenntnis von deren Geschäften ihrer Sorgfaltspflicht nachkommt.

14. Die Bedenken der Aufsichtsinstanzen zum **Konzentrationsrisiko** betreffen hauptsächlich die Aktivseite der Bilanz. Nach allgemeiner Praxis verlangen die Bankenaufsichtsbehörden von den Banken nicht nur, dass sie über Informationssysteme zur Erkennung von Konzentrationen innerhalb des Portfolios verfügen, sondern die meisten legen auch Limits fest, um das Engagement gegenüber einzelnen Kreditnehmern oder Gruppen miteinander verbundener Kreditnehmer zu begrenzen. Wenn eine Bank nicht genau weiss, wer ihre Kunden sind und welche Beziehungen unter den Kunden bestehen, kann sie ihr Konzentrationsrisiko nicht messen. Dies ist im Falle von miteinander verbundenen Kontrahenten und bei einer Kreditvergabe an in das Geschäft der Bank involvierte Schuldner von besonderer Bedeutung.

15. Auf der Passivseite ist das Konzentrationsrisiko eng mit dem Refinanzierungsrisiko verknüpft, insbesondere dem Risiko eines vorzeitigen und plötzlichen Mittelabzugs durch grosse Einleger, der verheerende Folgen für die Liquidität der Bank haben kann. Kleine Banken und Banken, die an den Grosshandels-Finanzmärkten weniger aktiv sind als grosse Banken, dürften einem höheren Refinanzierungsrisiko ausgesetzt sein. Bei der Analyse von Einlagenkonzentrationen muss eine Bank über die speziellen Merkmale ihrer Einleger informiert sein, d.h. sie muss nicht nur ihre Identität kennen, sondern auch wissen, inwieweit ihr Handeln von dem anderer Einleger abhängen kann. Es ist daher sehr wichtig, dass die für das Passivmanagement zuständigen Mitarbeiter kleiner Banken die grossen Einleger nicht nur kennen, sondern auch den Kontakt mit ihnen pflegen; andernfalls besteht die Gefahr, dass deren Mittel in kritischen Zeiten abgezogen werden.

16. Oft haben Kunden mehrere Konten bei derselben Bank, aber bei Niederlassungen in verschiedenen Ländern. Um das Reputations-, Compliance- und Rechtsrisiko im Zusammenhang mit solchen Konten wirksam handhaben zu können, sollte eine Bank in der Lage sein, erhebliche Guthaben und Vorgänge auf diesen Konten auf weltweit konsolidierter Basis zusammenzufassen und zu überwachen, unabhängig davon, ob es sich um ein Konto in der Bilanz, ein Konto ausserhalb der Bilanz, Vermögenswerte mit Verwaltungsauftrag oder ein Treuhandkonto handelt.

17. Sowohl der Basler Ausschuss für Bankenaufsicht als auch die Offshore-Gruppe von Bankenaufsichtsbehörden vertreten die uneingeschränkte Überzeugung, dass ein wirksames System der

Feststellung der Kundenidentität Bestandteil des Risikomanagements und der internen Kontrollen jeder Bank weltweit sein sollte. Die nationalen Aufsichtsinstanzen müssen dafür sorgen, dass die Banken Mindeststandards einhalten und über interne Kontrollen verfügen, die eine angemessene Identifizierung der Kunden gestatten. Freiwillige Verhaltenskodizes⁴ von Branchenverbänden können eine wertvolle Unterstützung der Aufsichtsrichtlinien bilden, indem sie den Banken zu geschäftlichen Belangen praktische Ratschläge geben. Sie können jedoch kein Ersatz für formelle Richtlinien der Aufsichtsbehörde sein.

III. Wesentliche Elemente der Standards für die Feststellung der Kundenidentität

18. Die Richtlinien des Basler Ausschusses für Bankenaufsicht über die Feststellung der Kundenidentität sind in drei Papieren enthalten, die die Entwicklung der Haltung der Aufsichtsinstanzen im Zeitverlauf widerspiegeln. Der Bericht *Verhütung des Missbrauchs des Bankensystems für die Geldwäsche*, der 1988 erschien, legt die wesentlichen ethischen Grundsätze dar und hält die Banken dazu an, wirksame Verfahren zur Feststellung der Identität ihrer Kunden zu schaffen, verdächtige Transaktionen zurückzuweisen und mit staatlichen Vollzugsorganen zusammenzuarbeiten. In den *Grundsätzen für eine wirksame Bankenaufsicht*, die 1997 herausgegeben wurden, wurde im breiteren Kontext der internen Kontrollen festgehalten, dass die Banken über angemessene Geschäftsgrundsätze, Geschäftspraktiken und Verfahrensweisen verfügen sollten, einschliesslich strenger Vorschriften über die Kenntnis der Kundenidentität; im besonderen sollten die Aufsichtsbehörden die Umsetzung der einschlägigen Empfehlungen der FATF unterstützen. Diese betreffen die Identifizierung der Kunden und das Aufbewahren von Unterlagen, erhöhte Sorgfalt der Finanzinstitute bei der Feststellung und Meldung verdächtiger Transaktionen sowie Massnahmen für den Verkehr mit Ländern, die unzulängliche Vorkehrungen zur Bekämpfung der Geldwäsche getroffen haben. In der 1999 herausgegebenen *Methodik der Grundsätze für eine wirksame Bankenaufsicht* werden die Grundsätze genauer ausgeführt, wobei eine Reihe zentraler und zusätzlicher Kriterien aufgelistet werden. (Anhang 1 enthält die einschlägigen Auszüge aus den *Grundsätzen* und der *Methodik*.)

19. Von allen Banken sollte verlangt werden, dass sie „über angemessene Geschäftsgrundsätze, Geschäftspraktiken und Verfahrensweisen verfügen, die einen hohen ethischen und professionellen Standard fördern und verhindern, dass die Banken - wissentlich oder unwissentlich - von kriminellen Elementen benutzt werden.“⁵ Bei der Gestaltung der Systeme zur Feststellung der Kundenidentität sollten die Banken bestimmte Schlüsselemente einbeziehen. Dabei sollten sie von ihren Risikomanagement- und Kontrollverfahren ausgehen und folgende Elemente berücksichtigen: 1) Regelungen für die Annahme von Kunden, 2) Feststellung der Kundenidentität, 3) kontinuierliche Überwachung von Hochrisikokonten und 4) Risikomanagement. Eine Bank sollte nicht nur die Identität ihrer Kunden feststellen, sondern auch die Kontobewegungen überwachen, um Transaktionen zu erkennen, die nicht den üblichen oder erwarteten Transaktionen für den betreffenden Kunden oder Kontotyp entsprechen. Die Feststellung der Kundenidentität muss ein Kernelement des Risikomanagements und der Kontrollverfahren einer Bank sein, und sie sollte durch eine regelmässige Überprüfung der Einhaltung und durch interne Revision ergänzt werden. Wie stark die Systeme zur Kundenidentifizierung über diese Kernelemente hinaus ausgebaut werden, sollte auf den jeweiligen Risikograd abgestimmt werden.

1. Regelungen für die Annahme von Kunden

20. Banken sollten klare Regelungen und Verfahren für die Annahme von Kunden entwickeln, u.a. eine Beschreibung der Kategorien von Kunden, die vermutlich ein überdurchschnittliches Risiko für eine Bank darstellen. Zu berücksichtigen sind dabei Faktoren wie Hintergrund des Kunden, Her-

⁴ Ein Beispiel eines Branchenkodex sind die „Global anti-money-laundering guidelines for Private Banking“ (auch „Wolfsberg-Prinzipien“ genannt); sie wurden im Oktober 2000 von zwölf grossen Banken mit bedeutendem Private-Banking-Geschäft erlassen.

⁵ *Methodik der Grundsätze für eine wirksame Bankenaufsicht*, Zentrales Kriterium 1.

kunftsland, öffentliche oder prominente Position, verbundene Konten, Geschäftstätigkeit und sonstige Risikoindikatoren. Die Regelungen und Verfahren sollten so abgestuft sein, dass bei Kunden mit höherem Risiko eine verstärkte Sorgfaltspflicht besteht. Beispielsweise genügen für Erwerbstätige mit einem geringen Kontoguthaben elementare Anforderungen bei der Kontoeröffnung. Die Regelungen für die Annahme von Kunden dürfen nicht so restriktiv sein, dass einer breiten Öffentlichkeit praktisch der Zugang zu Bankdienstleistungen versperrt wird, insbesondere nicht Personen, die finanziell oder sozial benachteiligt sind. Umgekehrt ist bei einer Person mit grossem Nettovermögen unklarer Herkunft sehr grosse Sorgfalt angebracht. Die Entscheidung, ob mit einem Kunden mit erhöhtem Risiko, z.B. einer politisch exponierten Person (s. Abschnitt 2.2.3 unten), eine Geschäftsbeziehung eingegangen werden soll, ist ausschliesslich auf der Ebene der Geschäftsleitung zu treffen.

2. Identifizierung der Kunden

21. Die Identifizierung eines Kunden ist ein zentrales Element der Sorgfaltspflicht. Für das vorliegende Papier gilt als Kunde:

- die natürliche oder juristische Person, die ein Konto bei der Bank hält, oder die Person, in deren Auftrag ein Konto gehalten wird (d.h. wirtschaftlich Berechtigte);
- die Begünstigten von Transaktionen professioneller Vermittler;
- jede natürliche oder juristische Person, die an einer Finanztransaktion beteiligt ist und die ein erhebliches Reputations- oder sonstiges Risiko für die Bank darstellen kann.

22. Banken sollten ein systematisches Verfahren für die Feststellung der Identität neuer Kunden schaffen und keine Geschäftsbeziehung eingehen, bevor die Identität eines neuen Kunden befriedigend abgeklärt ist.

23. Banken sollten „Geschäftsgrundsätze für die Identifizierung ihrer Kunden und deren Stellvertreter dokumentiert und durchgesetzt haben“.⁶ Am besten sind zur Überprüfung der Identität von Kunden solche Dokumente geeignet, die am schwierigsten illegal zu erlangen oder zu fälschen sind. Besondere Aufmerksamkeit ist bei Kunden aus einem anderen Land angebracht; in keinem Fall sollte eine Bank das Identifizierungsverfahren abkürzen, nur weil der neue Kunde nicht in der Lage ist, persönlich bei der Bank vorzusprechen. Die Bank sollte sich immer die Frage stellen, warum der Kunde ein Konto in einem fremden Land eröffnen will.

24. Zu Beginn der Geschäftsbeziehung ist die Feststellung der Identität der Kunden etwas Selbstverständliches. Damit die Unterlagen immer auf dem neuesten Stand und relevant sind, sollte eine Bank ihre bestehenden Akten regelmässig überprüfen.⁷ Eine Überprüfung ist z.B. angezeigt, wenn eine bedeutende Transaktion stattfindet oder wenn sich die Dokumentierungsstandards oder die Art und Weise, wie das Konto benutzt wird, erheblich ändern. Aber auch sobald eine Bank merkt, dass ihre Informationen über einen bestehenden Kunden nicht ausreichend sind, sollte sie dafür sorgen, dass alle einschlägigen Angaben so rasch wie möglich eingeholt werden.

25. Banken, die Dienstleistungen für vermögende Privatkunden anbieten („Private Banking“), sind dem Reputationsrisiko besonders ausgesetzt und sollten daher bei solchen Geschäften erhöhte Sorgfalt üben. Konten in diesem Privatkundengeschäft, das von seiner Natur her sehr vertraulich ist, können im Namen einer natürlichen Person, einer juristischen Person, eines Trusts, eines Vermittlers oder einer persönlichen Investmentgesellschaft eröffnet werden. In jedem Fall kann ein Reputationsrisiko entstehen, wenn die Bank nicht mit der gebotenen Sorgfalt die etablierten Verfahren zur Feststellung der Kundenidentität einhält. Alle neuen Kunden und neuen Konten sind, ausser vom zuständigen Kundenbetreuer, von mindestens einer weiteren Person von angemessenem Rang zu genehmigen. Wenn in einer Bank besondere Vorkehrungen zum Schutz der Vertraulichkeit von Privatkunden und deren Geschäften vorhanden sind, muss die Bank dennoch dafür sorgen, dass diese Kunden und ihre Geschäfte ebenso genau überprüft und überwacht werden können, z.B. durch Compliance-Beauftragte und Revisoren.

⁶ *Methodik der Grundsätze für eine wirksame Bankenaufsicht, Zentrales Kriterium 2.*

⁷ Die FATF überprüft derzeit die Anwendung neuer Standards der Kundenidentifizierung auf bestehende Konten.

26. Die Banken sollten klare Regelungen darüber erarbeiten, „welche Daten zur Kundenidentifizierung und zu den einzelnen Transaktionen wie lange aufbewahrt werden müssen“.⁸ Eine solche Praxis ist unabdingbar, damit eine Bank ihre Beziehung mit dem Kunden überwachen kann, die laufenden Geschäfte des Kunden versteht und nötigenfalls im Falle von Streitigkeiten, Gerichtsverfahren oder einer Untersuchung durch Finanzaufsichtsbehörden, die zu einem Strafverfahren führen kann, über Beweismaterial verfügt. Als Beginn und natürliche Fortsetzung des Identifikationsverfahrens sollte die Bank vom Kunden einen Identitätsausweis verlangen und eine Kopie davon noch mindestens fünf Jahre lang nach Schliessung des Kontos aufbewahren. Auch sämtliche Belege von Finanztransaktionen sind mindestens fünf Jahre lang aufzubewahren.

2.1 Allgemeine Anforderungen der Kundenidentifizierung

27. Eine Bank muss alle Angaben einholen, die notwendig sind, um einen neuen Kunden zu ihrer vollen Zufriedenheit zu identifizieren sowie den Zweck und die beabsichtigte Art der Geschäftsbeziehung zu erkennen. Art und Umfang der Informationen hängen davon ab, welcher Kategorie der Kunde angehört (Privat- oder Firmenkunde etc.) und welchen Umfang das Konto voraussichtlich hat. Die Aufsichtsinstanzen der einzelnen Länder sollten Richtlinien erlassen, um den Banken bei der Gestaltung der Identifikationsverfahren zu helfen. Die Arbeitsgruppe beabsichtigt, wichtige Elemente bei den Anforderungen der Kundenidentifizierung herauszuarbeiten.

28. Wenn ein Konto zwar eröffnet wird, dann aber unlösbare Überprüfungsprobleme in der Geschäftsbeziehung auftreten, sollte die Bank das Konto wieder schliessen und die Mittel an ihren Herkunftsort zurücküberweisen.⁹

29. Kommt die erste Einzahlung von einem Konto des Kunden bei einer anderen Bank, die die gleichen Standards bei der Feststellung der Kundenidentität einhält, mag dies zwar schon eine gewisse Beruhigung sein, doch sollte eine Bank dennoch daran denken, dass möglicherweise der vorherige Kundenbetreuer die Auflösung des Kontos verlangte, weil er Bedenken über zweifelhafte Aktivitäten hegte. Selbstverständlich haben Kunden das Recht, ihre Bank zu wechseln. Wenn eine Bank jedoch Grund zu der Annahme hat, dass eine andere Bank die Kontoeröffnung schon abgelehnt hat, sollte sie gegenüber dem betreffenden Kunden erhöhte Sorgfalt üben.

30. Eine Bank sollte nie einwilligen, ein Konto für einen Kunden zu eröffnen oder Geschäfte für ihn durchzuführen, wenn der Kunde auf Anonymität besteht oder einen fiktiven Namen angibt. Vertrauliche Nummernkonten¹⁰ dürfen ebenfalls nicht als anonyme Konten geführt werden, sondern sollten genau den gleichen Verfahren zur Feststellung der Kundenidentität unterworfen sein wie alle anderen Konten, auch wenn die Überprüfung nur von ausgewählten Mitarbeitern durchgeführt wird. Ein Nummernkonto darf zwar einen zusätzlichen Schutz für die Identität des Inhabers bieten, diese muss aber einem genügend grossen Kreis von Mitarbeitern bekannt sein, damit die erforderliche Sorgfalt geübt werden kann. Auf keinen Fall dürfen solche Konten dazu dienen, die Identität des Kunden vor dem Compliance-Beauftragten der Bank oder vor der Aufsichtsinstanz zu verbergen.

2.2 Besondere Identifikationsprobleme

31. Bei der Feststellung der Kundenidentität stellen sich mehrere wichtige Detailfragen. Eine Reihe von ihnen wird derzeit von der FATF im Rahmen einer allgemeinen Überprüfung ihrer 40 Empfehlungen untersucht, und die Arbeitsgruppe erkennt die Notwendigkeit an, ihre Arbeit auf die der FATF abzustimmen.

2.2.1 Trust-, Treuhand- und ähnliche Konten

32. Trust-, Treuhand- und ähnliche Konten können zur Umgehung von Kundenidentifikationsverfahren verwendet werden. In bestimmten Fällen mag es zwar zulässig sein, einen zusätzlichen

⁸ Methodik der Grundsätze für eine wirksame Bankenaufsicht, Zentrales Kriterium 2.

⁹ Vorbehalten bleiben gesetzliche Bestimmungen eines Landes über die Behandlung verdächtiger Transaktionen.

¹⁰ Bei einem Nummernkonto ist der Name des wirtschaftlich Berechtigten der Bank bekannt, wird jedoch in den späteren Unterlagen durch eine Kontonummer oder einen Codenamen ersetzt.

Schutzwall der Vertraulichkeit für unbescholtene Privatkunden zu schaffen, die wahren Verhältnisse sollten jedoch unbedingt bekannt sein. Die Bank sollte feststellen, ob ein Kunde den Namen eines anderen Kunden annimmt, als „Strohmann“ fungiert oder im Auftrag eines anderen als Trustee, Bevollmächtigter oder sonstiger Vermittler handelt. In einem solchen Fall ist es unerlässlich, einen zufriedenstellenden Nachweis der Identität etwaiger Vermittler und ihrer Auftraggeber sowie Angaben über die Art des Trusts oder sonstigen Verhältnisses einzuholen. Bei einem Trust ist insbesondere die Identität der Trustees, der Treugeber/Trustbegründer und der Begünstigten festzustellen.¹¹

2.2.2 Juristische Personen

33. Banken müssen besonders darauf achten, dass juristische Personen nicht von natürlichen Personen eingesetzt werden, um anonyme Konten zu halten. Persönliche Anlagevehikel wie „International Business Companies“ können eine ordnungsgemässe Identifizierung von Kunden oder wirtschaftlich Berechtigten erschweren. Eine Bank sollte sich Klarheit über die Struktur der Gesellschaft verschaffen, die Herkunft der Gelder ermitteln und die Identität der wirtschaftlich Berechtigten und der Verfügungsberechtigten feststellen.

34. Besondere Sorgfalt ist bei der Anknüpfung einer Geschäftsbeziehung mit einer Gesellschaft mit anonymen Aktionären oder Inhaberaktien angebracht. Die Identität der wirtschaftlichen Eigentümer aller solcher Gesellschaften ist überzeugend nachzuweisen. Besondere Wachsamkeit ist bei Gesellschaften am Platz, bei denen ein erheblicher Anteil des Kapitals aus Inhaberaktien besteht. Inhaberaktien können ohne Wissen der Bank den Eigentümer wechseln. Es obliegt der Bank, befriedigende Verfahren zur Überwachung der Identität bedeutender wirtschaftlicher Eigentümer zu schaffen. Die Bank muss zu diesem Zweck gegebenenfalls die Inhaberaktien immobilisieren, z.B. indem sie sie verwahrt.

2.2.3 Eingeführte Kunden

35. Die Verfahren zur Feststellung der Kundenidentität können sehr zeitaufwendig sein, und natürlich sollen die Unannehmlichkeiten für neue Kunden nach Möglichkeit beschränkt werden. In einigen Ländern ist es daher üblich geworden, dass die Banken sich bei an sie verwiesenen Geschäften auf die von anderen Banken oder von Agenten durchgeführten Verfahren verlassen. Dabei besteht die Gefahr, dass die Banken zu sehr auf die Sorgfalt dieser Agenten vertrauen. Eine Bank bleibt jedoch letztlich dafür verantwortlich, dass sie ihre Kunden und deren Geschäfte kennt, und sie darf sich nicht darauf verlassen, dass ein Agent - wie gut sein Ruf auch sein mag - der erforderlichen Sorgfaltspflicht nachgekommen ist. Insbesondere sollte sich eine Bank nicht auf Agenten verlassen, die schwächeren Standards für die Feststellung der Kundenidentität als die Bank selbst unterliegen oder die nicht bereit sind, Kopien ihrer Identifikationsunterlagen abzugeben.

36. Der Basler Ausschuss für Bankenaufsicht empfiehlt Banken, die Agenten einsetzen, sorgfältig zu prüfen, ob diese fachlich und charakterlich geeignet sind und ob sie den erforderlichen Sorgfaltspflichten gemäss den hier dargelegten Standards nachkommen. Letztlich ist immer die Bank dafür verantwortlich, dass sie ihre Kunden kennt. Eine Bank sollte anhand folgender Kriterien bestimmen, ob ein Agent verlässlich ist:¹²

- Er muss die Mindeststandards für die Sorgfalt bei der Feststellung der Kundenidentität einhalten, die in diesem Papier dargelegt werden.
- Er sollte ebenso strenge Verfahren zur Feststellung der Kundenidentität durchführen, wie es die Bank gegebenenfalls selbst getan hätte.
- Die Bank muss sich von der Verlässlichkeit der vom Agenten verwendeten Systeme zur Feststellung der Kundenidentität überzeugen.

¹¹ Die Begünstigten sind soweit möglich zu identifizieren, wenn sie bezeichnet sind. Die Begünstigten eines Trusts können allerdings nicht immer von Anfang an genau identifiziert werden. Beispielsweise kann es sich um ungeborene Kinder handeln, oder manchmal hängt die Begünstigung vom Eintreten bestimmter Ereignisse ab. Wenn die Begünstigten eine bestimmte Personengruppe sind, z.B. bei einem Pensionsfonds, wird vielleicht am besten wie bei einem Sammelkonto (s. Absatz 38/39) vorgegangen.

¹² Die FATF überprüft derzeit die Eignungskriterien für Agenten.

- Die Bank muss mit dem Agenten eine Vereinbarung abschliessen, wonach sie die Ausübung der Sorgfaltspflicht des Agenten jederzeit nachprüfen darf.
- Alle einschlägigen Informationen und sonstigen Unterlagen zur Identität des Kunden sind der Bank vom Agenten unverzüglich vorzulegen, und diese muss die vorgelegten Unterlagen sorgfältig prüfen. Diese Informationen müssen der Aufsichtsinstanz, der Finanzuntersuchungsbehörde oder dem entsprechenden staatlichen Vollzugsorgan zur Einsichtnahme zur Verfügung stehen, sofern die erforderliche gesetzliche Grundlage dafür besteht.

Darüber hinaus sollte eine Bank regelmässig überprüfen, ob ihre Agenten auch weiterhin den oben aufgeführten Kriterien entsprechen.

2.2.4 Von professionellen Vermittlern eröffnete Kundenkonten

37. Wenn eine Bank weiss oder Grund zu der Annahme hat, dass ein von einem professionellen Vermittler eröffnetes Kundenkonto für einen einzigen Kunden bestimmt ist, muss dieser Kunde identifiziert werden.

38. Oft führen Banken „Sammelkonten“, die von professionellen Vermittlern für Kunden wie z.B. Investmentfonds, Pensionsfonds oder Geldmarktfonds verwaltet werden. Darüber hinaus führen Banken Sammelkonten für Rechtsanwälte oder Börsenmakler; auf diesen liegen Mittel, die für ein breites Spektrum von Kunden verwahrt oder hinterlegt werden. Wenn die Mittel eines solchen Vermittlers in der Bank nicht zusammengefasst werden, sondern „Unterkonten“ bestehen, die jedem einzelnen wirtschaftlich Berechtigten zugeordnet werden können, müssen alle wirtschaftlich Berechtigten identifiziert werden.

39. Wenn die Mittel zusammengefasst werden, sollte die Bank dennoch versuchen, die wirtschaftlich Berechtigten festzustellen. Manchmal muss sie jedoch nicht über den Vermittler hinaus nachforschen, z.B. wenn dieser den gleichen Aufsichts- und Geldwäschebestimmungen und -verfahren unterliegt und insbesondere die gleichen Sorgfaltspflichten bei der Feststellung der Kundenidentität hat wie die Bank. Die Aufsichtsinstanz eines Landes sollte klare Richtlinien darüber erlassen, wann Banken nicht über den Vermittler hinaus nachforschen müssen. Banken sollten solche Konten nur dann akzeptieren, wenn der Vermittler nachweislich über ein solides Verfahren zur Feststellung der Kundenidentität und die nötigen Systeme und Kontrollen verfügt, um die Vermögenswerte auf dem Sammelkonto den einzelnen Berechtigten zuzuordnen. Wenn die Bank das Verfahren des Vermittlers beurteilt, sollte sie anhand der in Absatz 36 oben dargelegten Kriterien für Agenten, die der Bank Kunden zuführen, prüfen, ob ein professioneller Vermittler verlässlich ist.

40. Wenn der Vermittler der Bank die erforderlichen Angaben zu den wirtschaftlich Berechtigten nicht machen darf, weil er z.B. als Rechtsanwalt¹³ dem Berufsgeheimnis unterliegt, oder wenn er nicht einer Sorgfaltspflicht, die der hier beschriebenen entspricht, oder umfassenden gesetzlichen Bestimmungen zur Bekämpfung der Geldwäsche untersteht, dann sollte die Bank ihm nicht gestatten, ein Konto zu eröffnen.

2.2.5 Politisch exponierte Personen

41. Geschäftsbeziehungen mit Personen, die wichtige öffentliche Stellungen innehaben, und mit Personen oder Firmen, die offensichtlich mit diesen verbunden sind, können eine Bank einem erheblichen Reputations- und/oder Rechtsrisiko aussetzen. Als politisch exponiert gelten Personen, die prominente öffentliche Funktionen innehaben, u.a. Staats- und Regierungschefs, hochrangige Politiker, Beamte und Richter, hochrangige Offiziere, Mitglieder der Geschäftsleitung von staatlichen Unternehmen sowie wichtige Parteifunktionäre. Vor allem in Ländern, in denen Korruption verbreitet ist, besteht immer die Möglichkeit, dass solche Personen ihre Machtstellung missbrauchen, um sich durch Entgegennahme von Bestechungsgeldern, Veruntreuung etc. unrechtmässig zu bereichern.

42. Die Entgegennahme und Verwaltung von Mitteln, die korrupten politisch exponierten Personen gehören, schadet dem Ruf der Bank sehr und kann das Vertrauen der Öffentlichkeit in die ethischen Standards eines gesamten Finanzplatzes untergraben, da solche Fälle in der Regel ein

¹³ Die FATF überprüft derzeit die geltenden Verfahren zur Feststellung der Kundenidentität für Konten, die von Rechtsanwälten im Auftrag von Klienten eröffnet werden.

grosses Medieninteresse sowie starke politische Reaktionen auslösen, selbst wenn die unrechtmässige Herkunft der Vermögenswerte oft schwierig zu beweisen ist. Darüber hinaus kann sich die Bank mit kostspieligen Anzeigen und Arrestverfügungen von Vollzugs- oder Gerichtsbehörden konfrontiert sehen (einschl. internationaler Rechtshilfebegehren in Strafsachen), und sie könnte vom betroffenen Staat oder von den Opfern eines Regimes auf Schadensersatz verklagt werden. Unter bestimmten Umständen können die Bank und/oder ihre Mitarbeiter selbst wegen Geldwäsche angeklagt werden, wenn sie wussten oder wissen mussten, dass die Mittel aus Korruption oder einem anderen schweren Delikt stammten.

43. Einige Länder haben kürzlich ihre Gesetze und Verordnungen dahingehend geändert (oder sind dabei, es zu tun), dass die aktive Bestechung ausländischer Amtsträger strafbar ist, entsprechend dem einschlägigen internationalen Übereinkommen.¹⁴ In diesen Ländern wird die Bestechung ausländischer Amtsträger zu einem Ausgangsdelikt für Geldwäsche, und es gelten alle einschlägigen Gesetze und Verordnungen zur Bekämpfung der Geldwäsche (z.B. Meldung verdächtiger Transaktionen, Verbot, den Kunden zu warnen, internes Einfrieren der Mittel etc.). Aber selbst wenn eine solche explizite gesetzliche Grundlage im Strafrecht fehlt, ist es eindeutig unerwünscht und mit den berufsethischen Grundsätzen des Bankgeschäfts unvereinbar, eine Geschäftsbeziehung einzugehen oder aufrechtzuerhalten, wenn die Bank weiss oder Grund zu der Annahme hat, dass die Mittel aus Korruption oder Veruntreuung von Volksvermögen stammen. Es ist zwingend notwendig, dass eine Bank vor Eingehen einer Geschäftsbeziehung mit einer Person, von der sie vermutet, dass sie politisch exponiert ist, die Identität dieser Person sowie der Personen und Firmen, die offensichtlich mit ihr verbunden sind, genau prüft.

44. Eine Bank sollte von einem neuen Kunden ausreichende Informationen einholen und öffentlich verfügbare Informationen nachprüfen, um festzustellen, ob der betreffende Kunde eine politisch exponierte Person ist. Vor Eingehen einer Geschäftsbeziehung mit einer politisch exponierten Person sollte die Bank die Herkunft der Mittel untersuchen. Die Entscheidung über eine Kontoeröffnung ist auf der Stufe der Geschäftsleitung zu treffen.

2.2.6 Kunden, die nicht persönlich vorsprechen

45. Immer öfter werden Banken ersucht, Konten für Kunden zu eröffnen, die nicht persönlich bei der Bank vorsprechen. Bei ausländischen Kunden war das seit jeher häufig der Fall, aber mit der Ausbreitung von auf dem Postweg, telefonisch oder elektronisch erbrachten Bankdienstleistungen haben solche Anfragen erheblich zugenommen. Eine Bank sollte für Kunden, die nicht persönlich bei ihr vorsprechen, ebenso wirksame Identifizierungsverfahren und Standards der laufenden Überwachung anwenden wie für die Kunden, die für eine Besprechung zur Verfügung stehen. In diesem Zusammenhang stellt sich u.a. die Frage nach einer unabhängigen Überprüfung durch eine vertrauenswürdige Drittpartei. Dieses gesamte Thema der Feststellung der Identität von Kunden, die nicht persönlich bei der Bank vorsprechen, wird von der FATF diskutiert und wird auch im Rahmen der Änderung der EWG-Richtlinie von 1991 überprüft.

46. Ein typisches Beispiel für einen Kunden, der nicht persönlich zur Bank kommt, ist ein Kunde, der seine Bankgeschäfte mit Hilfe des Internets oder einer ähnlichen Technologie elektronisch durchführen will. Das elektronische Bankgeschäft („Electronic Banking“) umfasst derzeit eine breite Palette von Produkten und Dienstleistungen, die über Telekommunikationsnetze angeboten werden. Der unpersönliche und grenzenlose Charakter des Electronic Banking sowie die Geschwindigkeit der Transaktion führt zwangsläufig zu Problemen bei der Identifizierung der Kunden und bei der Überprüfung. Die Aufsichtsinstanzen erwarten von den Banken als grundlegende Politik, dass diese die verschiedenen Risiken neuer Technologien aktiv einschätzen und Verfahren zur Identifizierung von Kunden entwickeln, in denen diesen Risiken Rechnung getragen wird.¹⁵

47. Obwohl die Kunden unabhängig davon, ob sie persönlich vorsprechen oder nicht, die gleiche Dokumentation liefern können, ist es im Falle nicht persönlich vorsprechender Kunden schwieriger,

¹⁴ S. das Übereinkommen über die Bekämpfung der Bestechung ausländischer Amtsträger im internationalen Geschäftsverkehr (OECD-Konvention), angenommen von der OECD-Verhandlungskonferenz am 21. November 1997.

¹⁵ Die Arbeitsgruppe für elektronische Bankdienstleistungen des Basler Ausschusses für Bankenaufsicht gab im Mai 2001 Risikomanagement-Grundsätze für die elektronische Durchführung von Bankgeschäften heraus.

den Kunden und die Dokumentation abzugleichen. Die telefonische und elektronische Abwicklung von Bankgeschäften verschärft das Überprüfungsproblem noch zusätzlich.

48. Bei der Annahme von Geschäften von Kunden, die nicht persönlich vorsprechen:

- sollte die Bank für Kunden, die nicht persönlich bei ihr vorsprechen, ebenso wirksame Identifikationsverfahren anwenden wie für die Kunden, die für eine Besprechung zur Verfügung stehen;
- müssen spezielle und angemessene Massnahmen zur Minderung des höheren Risikos ergriffen werden.

Solche Risikominderungsmaßnahmen können beispielsweise sein:

- Beglaubigung der eingereichten Unterlagen;
- Anforderung zusätzlicher Unterlagen als Ergänzung zu denjenigen, die von persönlich vorschprechenden Kunden verlangt werden;
- unabhängiger Kontakt der Bank mit dem Kunden;
- Einführung durch eine Drittpartei, z.B. durch einen Agenten, der die in Absatz 36 aufgeführten Kriterien erfüllt;
- Forderung, dass die erste Einzahlung über ein auf den Namen des Kunden lautendes Konto bei einer anderen Bank erfolgen muss, die ähnlichen Sorgfaltspflichten bei der Feststellung der Kundenidentität unterliegt.

2.2.7 Korrespondenzbankensystem

49. In einem Korrespondenzbankensystem erbringt eine Bank für eine andere im Rahmen einer Vereinbarung Bankdienstleistungen. Korrespondenzkonten (Loro- und Nostro-Konten) werden von Banken in aller Welt verwendet; sie ermöglichen es den Banken, Geschäfte abzuwickeln und Dienstleistungen zu erbringen, die sie selbst nicht direkt anbieten. Besondere Sorgfalt ist bei Loro-Korrespondenzkonten angebracht, bei denen der Korrespondent Dienstleistungen in Ländern anbietet, in denen er nicht physisch präsent ist. Lässt eine Bank es an der gebotenen Sorgfalt bei solchen Konten mangeln, setzt sie sich den weiter oben beschriebenen Risiken aus, und sie muss vielleicht feststellen, dass sie Gelder hält und/oder weiterleitet, die aus Korruption, betrügerischen Machenschaften oder sonstigen Delikten stammen.

50. Eine Bank sollte genügend Informationen über ihre Korrespondenzbanken einholen, um volle Klarheit über deren Geschäfte zu erhalten. Dazu gehören u.a. Informationen über die Geschäftsleitung der Korrespondenzbank, die wichtigsten Geschäftsbereiche, ihre Standorte sowie ihre Vorkehrungen gegen Geldwäsche, den Zweck des Loro-Kontos, die Identität von Dritten, die eventuell die Korrespondenzbankdienstleistungen nutzen, sowie den Stand von Bankenregulierung und -aufsicht im Land der Korrespondenzbank. Banken sollten nur mit solchen ausländischen Banken Korrespondenzbankbeziehungen eingehen, die von den zuständigen Instanzen wirksam beaufsichtigt werden. Diese Banken sollten überdies über wirksame Grundsätze und Verfahren zur Annahme und Identifizierung von Kunden verfügen.

51. Vor allem sollte eine Bank keine Korrespondenzbankbeziehung zu einer Bank aufnehmen oder weiterführen, die ihren Sitz in einem Land hat, in dem sie nicht physisch präsent ist, und die keinem regulierten Finanzkonzern angehört (d.h. die ein reines Buchungszentrum ist). Besonders wachsam sollte eine Bank sein, wenn sie Korrespondenzbeziehungen mit Banken in Ländern fortführt, deren Standards für die Feststellung der Kundenidentität mangelhaft sind oder die im Kampf gegen die Geldwäsche als „nicht kooperativ“ eingestuft wurden. Eine Bank sollte darauf achten, dass ihre Korrespondenzbanken Sorgfaltspflichten nach den hier dargelegten Standards einhalten, und sie sollte selbst eine erhöhte Sorgfalt bei Transaktionen üben, die über die Korrespondenzkonten abgewickelt werden.

52. Besondere Beachtung sollte eine Bank dem Risiko schenken, dass ein Korrespondenzkonto eventuell direkt von Dritten für eigene Geschäfte genutzt wird („Durchlaufkonten“). Für solche Fälle gelten die gleichen Erwägungen wie für eingeführte Kunden, und sie sollten nach den Kriterien von Absatz 36 behandelt werden.

3. Fortlaufende Überwachung von Konten und Transaktionen

53. Die fortlaufende Überwachung ist ein wesentlicher Aspekt von wirksamen Verfahren für die Feststellung der Kundenidentität. Eine Bank kann ihr Risiko nur dann wirksam begrenzen und vermindern, wenn sie weiss, welche Vorgänge auf den Konten ihrer Kunden normal und plausibel sind, so dass sie Transaktionen erkennen kann, die vom üblichen Muster abweichen. Ohne eine solche Kenntnis dürfte es ihr nicht möglich sein, gegebenenfalls ihrer Pflicht zur Meldung verdächtiger Transaktionen an die zuständigen Behörden nachzukommen. Der Umfang der Überwachung muss risikogerecht sein. Eine Bank sollte über ein System verfügen, das ihr das Aufspüren ungewöhnlicher oder verdächtiger Vorgänge auf sämtlichen Konten ermöglicht. Dies kann z.B. durch Festlegen von Limits für eine bestimmte Gruppe oder Kategorie von Konten geschehen. Transaktionen, die diese Limits überschreiten, sind aufmerksam zu prüfen. Bestimmte Transaktionsarten sollten von der Bank als möglicher Hinweis darauf gedeutet werden, dass der Kunde ungewöhnliche oder verdächtige Geschäfte tätigt. Das können z.B. Transaktionen sein, die wirtschaftlich oder kaufmännisch scheinbar keinen Sinn ergeben oder die mit grossen Bareinzahlungen verbunden sind, die nicht den üblichen und erwarteten Transaktionen des Kunden entsprechen. Ein sehr hoher Kontoumsatz, der schlecht zur Höhe des Guthabens passt, kann darauf hindeuten, dass das Konto zur Geldwäsche benutzt wird. Beispiele verdächtiger Kontovorgänge können für die Banken sehr hilfreich sein; sie sollten daher Bestandteil der Massnahmen und Richtlinien eines Landes zur Bekämpfung der Geldwäsche sein.

54. Konten mit erhöhtem Risiko sollten besonders überwacht werden. Jede Bank sollte Schlüsselindikatoren für solche Konten bestimmen, unter Berücksichtigung des Hintergrunds des Kunden, wie z.B. sein Heimatland und die Herkunft der Mittel, der Art der involvierten Transaktionen sowie sonstiger Risikofaktoren. Bei Konten mit erhöhtem Risiko:

- sollte die Bank dafür sorgen, dass angemessene Managementinformationssysteme vorhanden sind, damit Mitglieder der Geschäftsleitung und Compliance-Beauftragte über die aktuellen Informationen verfügen, die sie zur Erkennung, Analyse und effektiven Überwachung von Kundenkonten mit erhöhtem Risiko benötigen. Gemeldet werden sollten beispielsweise fehlende Kontoeröffnungsunterlagen, ungewöhnliche Vorgänge auf einem Kundenkonto sowie eine Zusammenfassung der gesamten Beziehung eines Kunden zur Bank;
- sollten die für das Privatkundengeschäft zuständigen Mitglieder der Geschäftsleitung die persönlichen Verhältnisse der Kunden mit erhöhtem Risiko kennen und Drittinformationsquellen nicht vernachlässigen. Bedeutende Transaktionen solcher Kunden sind von einem Mitglied der Geschäftsleitung zu genehmigen;
- sollte eine Bank für Geschäftsbeziehungen mit politisch exponierten Personen und Prominenten oder mit Personen und Firmen, die offensichtlich mit diesen verbunden sind, eine klare Politik und interne Richtlinien, Verfahren und Kontrollen entwickeln und diese Geschäftsbeziehungen besonders aufmerksam überwachen.¹⁶ Da eine politisch exponierte Person nicht unbedingt von vornherein als solche erkannt wird und da bestehende Kunden im späteren Verlauf der Geschäftsbeziehung diesen Status erwerben können, sollten zu mindest die bedeutenderen Kunden regelmässig überprüft werden.

4. Risikomanagement

55. Wirksame Verfahren zur Feststellung der Kundenidentität umfassen eine angemessene Überwachung durch die Geschäftsleitung, Managementsysteme und -kontrollen, Aufgabentrennung, Schulung und Ähnliches. Das oberste Verwaltungsorgan der Bank sollte konsequent für ein wirksames Programm zur Feststellung der Kundenidentität sorgen, indem es die geeigneten Verfahren

¹⁶ Realistischerweise kann von der Bank nicht erwartet werden, dass sie jede entfernte familiäre, politische oder geschäftliche Verbindung eines ausländischen Kunden kennt oder untersucht. Ob einem Verdacht nachgegangen werden muss, hängt vom Umfang der Vermögenswerte oder des Umsatzes, von Transaktionsmustern, vom wirtschaftlichen Hintergrund, vom Ruf des Landes, von der Plausibilität der Erklärungen des Kunden etc. ab. Allerdings dürfen sich politisch exponierte Personen (oder vielmehr ihre Angehörigen und Freunde) nicht unbedingt als solche vorstellen, sondern eher als gewöhnliche (wenn auch reiche) Geschäftsleute, unter Verheimlichung der Tatsache, dass sie ihre hohe Stellung in einem legitimen Unternehmen ausschliesslich ihrer privilegierten Beziehung zum Amtsträger verdanken.

einführt und ihre Wirksamkeit sicherstellt. In der Bank sollte explizit festgehalten werden, wer die Verantwortung dafür trägt, dass die Grundsätze und Verfahren der Bank wirksam gehandhabt werden und dass sie als Minimum der Aufsichtspraxis des Landes entsprechen. Die Wege für die Meldung verdächtiger Transaktionen sind klar und schriftlich festzuhalten und dem gesamten Personal bekanntzugeben. Ferner sollten interne Verfahren bestehen, mit deren Hilfe beurteilt wird, ob etwaige gesetzliche Pflichten der Bank zur Meldung verdächtiger Transaktionen es erfordern, dass die Transaktion auch der zuständigen staatlichen Vollzugsbehörde und/oder der Aufsichtsinstanz gemeldet wird.

56. Die interne Revision und die Compliance-Stelle einer Bank erfüllen wichtige Aufgaben bei der Beurteilung und Sicherstellung der Einhaltung von Grundsätzen und Verfahren bei der Feststellung der Kundenidentität. Im allgemeinen nimmt die Compliance-Stelle eine unabhängige Beurteilung der eigenen Grundsätze und Verfahren der Bank vor, die auch die gesetzlichen und aufsichtlichen Vorschriften einschliesst. Sie sollte ferner dafür zuständig sein, die Arbeitsweise des Personals durch stichprobenweise Überprüfung der Einhaltung der Verfahren und Vorschriften sowie Überprüfung von Berichten über Ausnahmefälle und Abweichungen fortlaufend zu überwachen. So kann sie die Geschäftsleitung oder das oberste Verwaltungsorgan benachrichtigen, wenn sie zu dem Befund kommt, dass die Verfahren zur Feststellung der Kundenidentität nicht ernst genug genommen werden.

57. Die interne Revision spielt eine wichtige Rolle bei der unabhängigen Beurteilung des Risikomanagements und der Kontrollen. Sie bewertet regelmässig die effektive Einhaltung von Grundsätzen und Verfahren bei der Feststellung der Kundenidentität, einschliesslich der entsprechenden Personalschulung, und legt dem Geschäftsprüfungsausschuss des obersten Verwaltungsorgans oder einem ähnlichen Gremium darüber Rechenschaft ab. Die Geschäftsleitung sollte dafür sorgen, dass die interne Revision über Mitarbeiter mit entsprechenden Qualifikationen verfügt. Die internen Revisoren sollten ausserdem ihren Befunden und Kritiken aktiv nachgehen.

58. Jede Bank muss über ein festes Programm zur Schulung ihres Personals verfügen, damit dieses über die Verfahren zur Feststellung der Kundenidentität Bescheid weiss. Zeitplan und Inhalt der Schulung für die verschiedenen Mitarbeitergruppen müssen von der Bank auf ihre Bedürfnisse abgestimmt werden. Der Schwerpunkt der Schulung ist für neue Mitarbeitende, Mitarbeitende im Kundenverkehr und Kontaktpersonen für Neukunden sowie Mitarbeitende in der Compliance-Stelle jeweils unterschiedlich. Neue Mitarbeitende sollten über die Bedeutung der Feststellung der Kundenidentität und die wichtigsten Erfordernisse in der Bank aufgeklärt werden. Mitarbeitende, die im Kundenverkehr tätig sind und direkt mit der Öffentlichkeit Kontakt haben, sollten darin geschult werden, die Identität neuer Kunden zu prüfen, ständig die gebotene Sorgfalt bei der Behandlung von Konten bestehender Kunden zu üben und verdächtige Transaktionsmuster zu entdecken. Mit Hilfe regelmässiger Auffrischkurse sollten die Mitarbeitenden an ihre Verantwortung erinnert und über neue Entwicklungen auf dem laufenden gehalten werden. Alle betroffenen Mitarbeitenden müssen genau wissen, dass die Grundsätze zur Feststellung der Kundenidentität notwendig sind und konsequent umgesetzt werden müssen. Eine Unternehmenskultur in der Bank, die dieses Bewusstsein fördert, ist der Schlüssel zu einer erfolgreichen Umsetzung.

59. In zahlreichen Ländern haben auch die externen Revisoren eine wichtige Aufgabe bei der Überwachung der internen Kontrollen und Verfahren der Banken und bei der Bestätigung, dass diese der Aufsichtspraxis entsprechen.

IV. Rolle der Aufsichtsbehörden

60. Die Aufsichtsinstanzen der einzelnen Länder sollten, gestützt auf bestehende internationale Standards, eine Aufsichtspraxis bezüglich der Systeme der Banken zur Feststellung der Kundenidentität entwickeln. Die in diesem Papier vorgelegten zentralen Elemente sollten ihnen bei der Gestaltung oder Verbesserung ihrer Praxis klare Leitlinien geben.

61. Die Aufsichtsinstanzen sollten den Banken nicht nur die Grundelemente vorgeben, sondern auch darauf achten, dass sie bei der Feststellung der Kundenidentität solide Verfahren anwenden und stets ethische und professionelle Standards einhalten. Die Aufsichtsinstanz sollte darauf achten, dass angemessene interne Kontrollen vorhanden sind und dass die Banken gesetzliche und aufsichtliche Richtlinien einhalten. Das Aufsichtsverfahren sollte nicht nur eine Überprüfung von Grundsätzen und

Verfahren umfassen, sondern auch eine Prüfung von Kundenakten und Stichproben einiger Konten. Die Aufsichtsinstanz sollte immer das Recht auf Einsichtnahme in alle Unterlagen von Konten in ihrem Land haben, ebenso in etwaige Analysen der Bank zum Aufspüren von ungewöhnlichen oder verdächtigen Transaktionen.

62. Die Aufsichtsinstanz hat nicht nur die Pflicht, für hohe Standards bei der Feststellung der Kundenidentität in den Banken zum Schutz von deren Sicherheit und Solidität zu sorgen, sondern auch, die Integrität des gesamten Bankensystems des Landes zu schützen.¹⁷ Die Aufsichtsinstanz sollte klarstellen, dass sie angemessene Massnahmen - die nötigenfalls sehr streng und öffentlich sein können - gegen Banken und deren Mitarbeitende ergreifen wird, die nachweislich ihre eigenen internen Verfahren und die regulatorischen Vorschriften missachten. Die Aufsichtsinstanz sollte ausserdem dafür sorgen, dass die Banken auf Transaktionen achten und ihnen besondere Aufmerksamkeit schenken, die Länder mit als unzulänglich angesehenen Standards betreffen. Die FATF und einige staatliche Stellen haben Listen von Ländern und Territorien erstellt, deren Rechts- und Verwaltungssysteme als nicht den internationalen Standards im Kampf gegen die Geldwäsche entsprechend eingestuft werden. Solche Befunde sollten in den Grundsätzen und Verfahren einer Bank berücksichtigt werden.

V. Umsetzung von Standards für die Feststellung der Kundenidentität im grenzüberschreitenden Geschäft

63. Aufsichtsinstanzen in aller Welt sollten nach Möglichkeit darauf achten, dass die Standards für die Feststellung der Kundenidentität, die sie für ihr Land entwickeln und umsetzen, internationalen Standards entsprechen, um Aufsichtsarbitrage zu verhindern und die Integrität des Bankensystems auf nationaler und internationaler Ebene zu wahren. Die Umsetzung und Beurteilung solcher Standards zeigen, in welchem Masse Aufsichtsinstanzen gewillt sind, untereinander praktisch zusammenzuarbeiten, und Banken in der Lage sind, Risiken konzernweit zu kontrollieren. Dies ist für Banken und Aufsichtsbehörden gleichermaßen eine Herausforderung.

64. Aufsichtsinstanzen verlangen von Bankkonzernen die Anwendung anerkannter Mindeststandards bei der Feststellung der Kundenidentität sowohl im inländischen als auch im internationalen Geschäft. Internationale Bankenaufsicht kann nur auf konsolidierter Basis wirksam durchgeführt werden, und das Reputationsrisiko und die anderen Risiken des Bankgeschäfts kennen keine Landesgrenzen. Das jeweilige Mutterinstitut muss seine Grundsätze und Verfahren den ausländischen Niederlassungen und Töchtern, einschliesslich Nichtbanken wie z.B. Treuhandgesellschaften, bekanntmachen und über ein Routineverfahren verfügen, um die Einhaltung der Standards sowohl des Herkunfts- als auch des Aufnahmelandes zu prüfen, damit sein System weltweit funktioniert. Die Verfahren zur Prüfung der Einhaltung wiederum werden von den externen Revisoren und der Aufsichtsinstanz überprüft. Es ist daher wichtig, dass die Unterlagen über die Kundenidentität ordnungsgemäss abgelegt und zur Einsichtnahme verfügbar sind. Was die Überprüfung der Einhaltung der Standards für die Feststellung der Kundenidentität betrifft, sollten Aufsichtsinstanzen und externe Revisoren in der Regel die Systeme und Kontrollen sowie stichprobenweise Kundenkonten und -transaktionen überprüfen.

65. Auch bei einer kleinen ausländischen Niederlassung sollte ein Mitglied der Geschäftsleitung direkt dafür verantwortlich sein, dass ihr zuständiges Personal in den Verfahren zur Feststellung der Kundenidentität, die den Standards im Herkunfts- wie im Aufnahmeland entsprechen, geschult wird und sie einhält. Diese Person trägt die Hauptverantwortung, sie sollte aber von den internen Revisoren und Compliance-Beauftragten des Hauptsitzes und gegebenenfalls der Niederlassung unterstützt werden.

66. Wenn die Mindestanforderungen im Herkunfts- und im Aufnahmeland unterschiedlich sind, sollten ausländische Zweigstellen und Töchter die höheren Standards anwenden. Im allgemeinen sollte nichts eine Bank daran hindern, höhere Standards als die vor Ort geltenden Mindeststandards

¹⁷ Viele Aufsichtsbehörden sind darüber hinaus verpflichtet, verdächtige, ungewöhnliche oder illegale Transaktionen, die sie beispielsweise bei einer Prüfung vor Ort entdeckt haben, zu melden.

einzuhalten. Wenn jedoch die Gesetze und Vorschriften eines Landes (insbesondere das Bankgeheimnis) die Umsetzung von im Herkunftsland geltenden strengeren Standards für die Feststellung der Kundenidentität verbieten, sollte die Aufsichtsinstanz des Aufnahmelandes auf eine Änderung solcher Gesetze und Vorschriften hinwirken. Unterdessen müssen sich die ausländischen Niederlassungen und Töchter an die Standards des Aufnahmelandes halten; sie sollten jedoch sicherstellen, dass der Hauptsitz bzw. das Mutterinstitut und die Aufsichtsinstanz ihres Herkunftslandes über den Unterschied genau informiert sind.

67. Für kriminelle Elemente dürften Rechtsordnungen attraktiv sein, für die solche Einschränkungen gelten. Eine Bank sollte sich daher des erhöhten Reputationsrisikos bewusst sein, das sie bei einer Geschäftstätigkeit in solchen Ländern eingeht. Die Mutterbank sollte ein Verfahren für die Überprüfung der Anfälligkeit der einzelnen Geschäftseinheiten schaffen und gegebenenfalls zusätzliche Sicherheitsvorkehrungen treffen. Im Extremfall sollte die Aufsichtsinstanz erwägen, den Banken, die in solchen Ländern tätig sind, zusätzliche Kontrollen aufzuerlegen und sie vielleicht sogar zu einem Rückzug anzuhalten.

68. Bei Prüfungen vor Ort sollten die Aufsichtsinstanz des Herkunftslandes oder die Revisoren ungehindert nachprüfen können, inwieweit die Geschäftseinheiten die Grundsätze und Verfahren für die Feststellung der Kundenidentität einhalten. Dies erfordert eine Überprüfung von Kundenakten sowie Stichprobenprüfungen von Konten. Die Aufsichtsinstanz des Herkunftslandes sollte Zugang zu Informationen über zufällig ausgewählte Kundenkonten haben, so dass sie die Anwendung der Standards für die Kundenidentifizierung und die Risikomanagement-Praxis angemessen beurteilen kann; gesetzliche Bestimmungen über das Bankgeheimnis sollten kein Hindernis sein. Wenn die Aufsichtsinstanz des Herkunftslandes die konsolidierte Meldung von Einlagen- oder Schuldnerkonzentrationen oder die Meldung von im Auftrag von Dritten verwalteten Vermögen fordert, sollte dem nichts im Wege stehen. Darüber hinaus kann die Aufsichtsinstanz des Herkunftslandes im Rahmen der Überwachung von Einlagenkonzentrationen bzw. des Refinanzierungsrisikos im Falle des Abzugs dieser Einlagen Erheblichkeitstests anwenden und Schwellenwerte festlegen; überschreitet dann die Einlage eines Kunden einen bestimmten Prozentsatz der Bilanzsumme, muss die Bank dies der Aufsichtsinstanz melden. Es sind jedoch Sicherheitsvorkehrungen notwendig, damit Informationen über einzelne Konten ausschliesslich für rechtmässige Aufsichtszwecke verwendet werden und vom Empfänger angemessen geschützt werden können. Diesbezüglich wäre eine Erklärung über die gegenseitige Zusammenarbeit¹⁸ hilfreich, die den Informationsaustausch zwischen den beiden Aufsichtsinstanzen erleichtert.

69. In bestimmten Fällen kann ein ernstlicher Konflikt entstehen zwischen den Grundsätzen für die Feststellung der Kundenidentität, die der Mutterbank von ihrer Aufsichtsinstanz auferlegt werden, und dem, was einer ausländischen Niederlassung gestattet ist. Beispielsweise können Gesetze des Aufnahmelandes Prüfungen durch Compliance-Beauftragte oder interne Revisoren des Mutterinstituts oder durch die Aufsichtsinstanz des Herkunftslandes verbieten, oder sie können es Bankkunden erlauben, fiktive Namen zu verwenden oder Agenten oder Vermittler vorzuschieben, die die Identität ihrer Kunden nicht offenlegen dürfen. In solchen Fällen sollte sich die Aufsichtsinstanz des Herkunftslandes mit der des Aufnahmelandes in Verbindung setzen, um abzuklären, ob tatsächlich echte gesetzliche Hindernisse bestehen und ob sie auch extraterritorial gelten. Erweisen sie sich als unüberwindbar und gibt es keine befriedigenden Alternativen, sollte die Aufsichtsinstanz des Herkunftslandes der des Aufnahmelandes klarmachen, dass die Bank selbst die Entscheidung treffen oder von ihrer Herkunftsland-Aufsicht dazu gezwungen werden kann, die betreffende Geschäftsstelle zu schliessen. Letztlich sollten die Vorkehrungen für solche Prüfungen vor Ort eine Beurteilung ermöglichen, die die Aufsichtsinstanz des Herkunftslandes zufriedenstellt. Erklärungen über die Zusammenarbeit oder Grundsatzabkommen, in denen das Vorgehen geregelt wird, können hilfreich sein. Der Zugang der Aufsichtsinstanz des Herkunftslandes zu Informationen sollte so wenig wie möglich behindert werden; als Minimum sollte diese Instanz freien Zugang zu den allgemeinen Grundsätzen und Verfahren der Bank hinsichtlich der Sorgfaltspflicht bei der Feststellung der Kundenidentität und des Vorgehens bei einem Verdacht haben.

¹⁸ S. das Papier *Essential elements of a statement of cooperation between banking supervisors* des Basler Ausschusses für Bankenaufsicht (Mai 2001).

Anhang 1: **Auszug aus der** **Methodik der Grundsätze für eine wirksame Bankenaufsicht**

Grundsatz 15: Die Bankenaufsichtsbehörden müssen sich überzeugen, dass die Banken über angemessene Geschäftsgrundsätze, Geschäftspraktiken und Verfahrensweisen verfügen, einschliesslich strenger Vorschriften über die Kenntnis der Kundenidentität, die einen hohen ethischen und professionellen Standard im Finanzsektor fördern und verhindern, dass die Bank - wissentlich oder unwissentlich - von kriminellen Elementen benutzt wird.

Zentrale Kriterien

1. Die Aufsichtsbehörde überzeugt sich davon, dass die Banken über angemessene Geschäftsgrundsätze, Geschäftspraktiken und Verfahrensweisen verfügen, die einen hohen ethischen und professionellen Standard fördern und verhindern, dass die Banken – wissentlich oder unwissentlich – von kriminellen Elementen benutzt werden. Darunter fallen die Vorbeugung gegen und Erkennung von kriminellen oder betrügerischen Machenschaften und die Meldung an die zuständigen Behörden, wenn solche Machenschaften vermutet werden.
2. Die Aufsichtsbehörde überzeugt sich davon, dass die Banken im Rahmen ihrer Bemühungen zur Bekämpfung der Geldwäsche Geschäftsgrundsätze für die Identifizierung ihrer Kunden und deren Stellvertreter dokumentiert und durchgesetzt haben. Es ist klar geregelt, welche Daten zur Kundenidentifizierung und zu den einzelnen Transaktionen wie lange aufbewahrt werden müssen.
3. Die Aufsichtsbehörde überzeugt sich davon, dass die Banken formelle Verfahren für das Erkennen potentiell verdächtiger Transaktionen eingeführt haben. Darunter fallen beispielsweise auch zusätzliche Ermächtigungen im Falle von Einzahlungen oder Abhebungen grosser Barbeträge o.ä. sowie spezielle Verfahren für ungewöhnliche Transaktionen.
4. Die Aufsichtsbehörde überzeugt sich davon, dass die Banken jeweils einen leitenden Angestellten bestimmen, der ausdrücklich dafür zuständig ist, dass die Geschäftsgrundsätze und Verfahrensweisen zumindest den lokalen gesetzlichen und aufsichtsbehördlichen Anforderungen zur Bekämpfung der Geldwäsche entsprechen.
5. Die Aufsichtsbehörde vergewissert sich, dass die Banken über klare, allen Mitarbeitern bekannte Verfahrensweisen verfügen, wonach verdächtige Transaktionen dem leitenden Angestellten gemeldet werden müssen, der für die Einhaltung der geltenden Bestimmungen zur Geldwäschebekämpfung zuständig ist.
6. Die Aufsichtsbehörde überzeugt sich davon, dass die Banken Kommunikationskanäle für die Meldung von Problemen eingerichtet haben, so dass sowohl die Geschäftsleitung als auch eine interne Sicherheitsfunktion in Kenntnis gesetzt werden.
7. Neben einer Anzeige bei den zuständigen Strafverfolgungsbehörden melden die Banken verdächtige Machenschaften oder Betrugsfälle, die ihre Sicherheit, Solidität oder ihren Ruf bedrohen, auch der Aufsichtsbehörde.
8. Gesetze, Vorschriften und/oder die Geschäftsgrundsätze der Banken sorgen dafür, dass ein Mitarbeiter, der verdächtige Transaktionen in gutem Glauben dem zuständigen leitenden Angestellten, der internen Sicherheitsfunktion oder direkt der zuständigen Behörde meldet, nicht dafür haftbar gemacht werden kann.
9. Die Aufsichtsbehörde überprüft periodisch, dass die Massnahmen der Banken zur Bekämpfung der Geldwäsche und die entsprechenden Abläufe zur Vorbeugung gegen sowie Erkennung und Meldung von Betrugsfällen ausreichen. Die Aufsichtsbehörde verfügt über ausreichende Durchsetzungsbefugnisse, um (durch ein aufsichts- und/oder strafrechtliches Verfahren) gegen eine Bank, die ihre Pflicht zur Bekämpfung der Geldwäsche nicht wahrnimmt, vorzugehen.

10. Die Aufsichtsbehörde kann mit inländischen oder ausländischen Aufsichtsbehörden des Finanzsektors Informationen über vermutete oder tatsächliche kriminelle Machenschaften direkt oder indirekt austauschen.
11. Die Aufsichtsbehörde überzeugt sich davon, dass die Banken eine Grundsatzerklärung über Ethik und professionelles Verhalten abgegeben haben, die allen Mitarbeitern genau bekannt ist.

Zusätzliche Kriterien

1. Die Gesetze und/oder Vorschriften berücksichtigen weltweit gültiges verantwortungsbewusstes Geschäftsgebaren wie z.B. die vierzig wichtigen Empfehlungen der Financial Action Task Force aus dem Jahre 1990 (die 1996 überarbeitet wurden).
2. Die Aufsichtsbehörde vergewissert sich, dass den Mitarbeitern der Banken die nötigen Kenntnisse im Bereich der Erkennung von und Vorbeugung gegen Geldwäsche vermittelt werden.
3. Die Aufsichtsbehörde ist gesetzlich verpflichtet, verdächtige Transaktionen den zuständigen Strafverfolgungsbehörden zu melden.
4. Die Aufsichtsbehörde kann mit den zuständigen Justizbehörden Informationen über vermutete oder tatsächliche kriminelle Machenschaften direkt oder indirekt austauschen.
5. Falls keine andere Stelle dafür zuständig ist, verfügt die Aufsichtsbehörde über eigene Mitarbeiter mit Sachkenntnis im Bereich Finanzbetrügereien und Pflicht zur Geldwäschebekämpfung.

Anhang 2: Auszug aus den Empfehlungen der FATF

C. Die Rolle des Finanzwesens bei der Bekämpfung der Geldwäsche

Kundenidentifizierung und Aufzeichnungen

10. Finanzinstitute sollten keine anonymen Konten bzw. auf offensichtlich fiktive Namen lautende Konten führen: Sie sollten (durch Gesetze, Vorschriften, Abkommen zwischen Aufsichtsbehörden und Finanzinstituten oder selbstregelnde Abkommen zwischen Finanzinstituten) dazu verpflichtet sein, ihre Kunden auf der Grundlage offizieller oder sonstiger zuverlässiger Ausweispapiere zu identifizieren und die Identität ihrer Gelegenheits- bzw. Stammkunden aufzuzeichnen, wenn Geschäftsbeziehungen hergestellt oder Geschäfte abgewickelt werden (im besonderen bei der Eröffnung von Konten oder Sparbüchern, der Abwicklung von Treuhandgeschäften, der Miete von Schliessfächern und der Durchführung bedeutender Bargeschäfte).

Um den Identifizierungsanforderungen bezüglich juristischer Personen nachzukommen, sollten die Finanzinstitute notfalls Massnahmen ergreifen:

- i) um die juristische Existenz und Struktur des Kunden zu überprüfen, indem entweder aus einem öffentlichen Register oder vom Kunden selbst oder aus beiden Quellen der Beweis für die Eintragung als Gesellschaft erhalten wird, einschliesslich Daten über den Namen des Kunden, Rechtsform, Anschrift, Geschäftsführer und Bestimmungen, die die das Unternehmen bindenden Handelsvollmachten regeln;
 - ii) um zu überprüfen, ob eine Person, die angibt, im Namen des Kunden zu handeln, wirklich dazu ermächtigt ist, und um die Identität dieser Person festzustellen.
11. Finanzinstitute sollten angemessene Massnahmen ergreifen, um Informationen über die wirkliche Identität der Personen, in deren Namen ein Konto eröffnet wird oder ein Geschäft abgewickelt wird, zu erhalten, wenn Zweifel bestehen, ob diese Kunden wirklich in ihrem eigenen Namen handeln, z.B. im Fall von Unternehmen (d.h. Institute, Gesellschaften, Stiftungen, Trusts usw.), die in dem Land, in dem sich ihr Sitz befindet, keine gewerblichen bzw. industriellen Aktivitäten oder sonstigen Handelsgeschäfte ausüben.
12. Finanzinstitute sollten alle nötigen Aufzeichnungen über Geschäfte im In- und Ausland mindestens fünf Jahre aufbewahren, um Informationsanfragen von zuständigen Behörden ohne Verzug nachkommen zu können. Diese Aufzeichnungen müssen ausreichend sein, um die Rekonstruktion individueller Geschäfte (einschl. der eventuell involvierten Devisenarten und -beträge) zu ermöglichen und wenn nötig als Beweismaterial für die Ahndung verbrecherischen Verhaltens eingesetzt werden zu können.
- Finanzinstitute sollten Aufzeichnungen über die Identität der Kunden (z.B. Kopien oder Aufzeichnungen der offiziellen Ausweispapiere wie Pässe, Personalausweise, Führerscheine oder ähnliche Unterlagen), Kontoauszüge und Geschäftskorrespondenz mindestens fünf Jahre nach der Schliessung des Kontos aufbewahren.
- Diese Aufzeichnungen sollten den zuständigen nationalen Behörden im Rahmen strafrechtlicher Ermittlungen und Verfahren zur Verfügung stehen.
13. Länder sollten besonders die Möglichkeiten beachten, die in neuen oder sich entwickelnden Technologien enthalten sind und die Anonymität fördern, und notfalls Massnahmen ergreifen, um ihren Einsatz in Geldwäscheprojekten zu verhindern.

Höhere Sorgfalt der Finanzinstitute

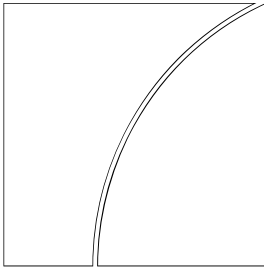
14. Die Finanzinstitute sollten besonders alle komplexen, ungewöhnlich bedeutenden Geschäfte sowie alle unüblichen Geschäftsschemen, die keinen klar ersichtlichen wirtschaftlichen oder gesetzesmässigen Zweck verfolgen, beachten. Der Hintergrund und der Zweck dieser Geschäfte sollte gegebenenfalls untersucht werden, die Ergebnisse sollten schriftlich fest-

- gelegt und erhältlich sein, um Aufsichtsbehörden, Abschlussprüfern und Vollzugsbehörden zu helfen.
15. Wenn Finanzinstitute den Verdacht haben, dass Kapital aus einer strafbaren Handlung stammen könnte, sollten sie dazu gezwungen sein, den zuständigen Behörden diesen Verdacht zu melden.
 16. Die Finanzinstitute, deren Leiter, Führungskräfte und Arbeitnehmer sollten durch gesetzliche Bestimmungen gegen strafrechtliche oder zivilrechtliche Haftpflicht aus dem Verstoß gegen eine vertraglich oder gesetzlich oder durch Statuten bzw. die Verwaltung auferlegte Begrenzung der Enthüllung von Informationen geschützt werden, wenn sie den zuständigen Behörden ihren Verdacht gutgläubig melden, auch wenn sie nicht genau wissen, um welche strafbare Handlung es sich handelt, und ohne Rücksicht darauf, ob wirklich eine strafbare Handlung vorliegt.
 17. Die Finanzinstitute, deren Leiter, Führungskräfte und Arbeitnehmer sollten ihre Kunden nicht warnen bzw. gegebenenfalls nicht warnen dürfen, wenn Daten über sie den zuständigen Behörden gemeldet werden.
 18. Die Finanzinstitute, die ihren Verdacht melden, sollten die Anweisungen der zuständigen Behörden beachten.
 19. Die Finanzinstitute sollten Programme zur Bekämpfung der Geldwäsche entwickeln. Diese Programme sollten mindestens Folgendes umfassen:
 - i) Entwicklung interner Politiken, Verfahren und Kontrollen, einschliesslich der Bestimmung von mit der Einhaltung beauftragten Personen auf der Führungsebene, und geeigneter Verfahren, die bei der Personalauswahl höchste Ansprüche gewährleisten.
 - ii) Weiter- und Fortbildungsprogramm für die Mitarbeiter.
 - iii) Eine interne Revisionsstelle zur Überprüfung der Wirksamkeit des Systems.

Comité de Bâle sur le
contrôle bancaire

374

Bulletin CFB 44/2003



Devoir de diligence des banques au sujet de la clientèle

Octobre 2001



BANQUE DES RÈGLEMENTS INTERNATIONAUX

Groupe de travail sur les activités bancaires transfrontières

Co-Présidents:

Charles Freeland, Secrétaire Général Adjoint du Comité de Bâle sur le contrôle bancaire

Colin Powell, Président du Groupe offshore des autorités de contrôle bancaire et Président de la Jersey Financial Services Commission

Bermuda Monetary Authority

Cayman Islands Monetary Authority

Banque de France/Commission bancaire

Bundesaufsichtsamt für das Kreditwesen, Allemagne

Guernsey Financial Services Commission

Banca d'Italia

Agence de surveillance financière, Japon

Commission de surveillance du secteur financier,
Luxembourg

Monetary Authority of Singapore

Commission fédérale des banques, Suisse

Financial Services Authority, Royaume-Uni

Board of Governors of the Federal Reserve System

Federal Reserve Bank of New York

Office of the Comptroller of the Currency

Secrétariat

M. D. Munro Sutherland

M. John Bourbon
M^{me} Anna McLean

M. Laurent Ettori

M. Jochen Sanio
M. Peter Kruschel

M. Peter G. Crook (jusqu'à avril 2001)
M. Philip Marr (depuis avril 2001)

M. Giuseppe Godano

M. Kiyotaka Sasaki (jusqu'à juillet 2001)
M. Hisashi Ono (depuis juillet 2001)

M. Romain Strock

M^{me} Foo-Yap Siew Hong
M. Teo Lay Har

M. Daniel Zuberbühler
M^{me} Dina Balleyguier

M. Richard Chalmers

M. William Ryback

M^{me} Nancy Bercovici

M. Jose Tuya
M^{me} Tanya Smith

M. Andrew Khoo

Table des matières

I.	Introduction	1
II.	Importance des normes CC pour les autorités de contrôle et les banques	2
III.	Éléments essentiels des normes CC	4
1.	Politique d'acceptation des nouveaux clients	4
2.	Identification de la clientèle	5
2.1	Exigences générales d'identification	6
2.2	Aspects particuliers de l'identification	6
2.2.1	Comptes de fiducie et de mandataire	6
2.2.2	Personnes morales	6
2.2.3	Clientèle recommandée	7
2.2.4	Comptes clients ouverts par des intermédiaires professionnels	7
2.2.5	Personnes politiquement exposées (PPE)	8
2.2.6	Clients à distance	9
2.2.7	Banques correspondantes	9
3.	Surveillance continue des comptes et transactions	10
4.	Gestion des risques	11
IV.	Rôle des autorités de contrôle	12
V.	Mise en œuvre des normes CC dans un contexte transfrontière	12
	Annexe 1: Extraits de <i>Méthodologie des Principes fondamentaux</i>	14
	Annexe 2: Extraits des recommandations du GAFI	16

Devoir de diligence des banques au sujet de la clientèle

I. Introduction

1. Les autorités de contrôle du monde entier admettent de plus en plus qu'il est essentiel, pour les banques de leur juridiction, de disposer de contrôles et procédures appropriés leur permettant de savoir avec qui elles traitent. Un aspect majeur de ces contrôles réside dans un devoir de diligence adéquat au sujet de la clientèle nouvelle et existante. Si ce devoir de diligence fait défaut, les banques peuvent être amenées à subir un préjudice financier substantiel lié au risque d'atteinte à la réputation, au risque opérationnel, au risque juridique et au risque de concentration.

2. En examinant les résultats d'une étude interne sur les activités bancaires transfrontières en 1999, le Comité de Bâle a décelé des lacunes, dans de nombreux pays, concernant les politiques suivies par les banques en matière de connaissance clientèle (CC). D'un point de vue prudentiel, ces approches présentent, dans certains cas, d'importantes déficiences et sont inexistantes dans d'autres; même dans les pays dotés de marchés financiers bien développés, elles sont plus ou moins rigoureuses. Le Comité a donc demandé au Groupe de travail sur les activités bancaires transfrontières¹ d'analyser les procédures CC actuellement en vigueur et de définir des normes dont l'application par les banques serait recommandée pour tous les pays. Le document produit a été publié aux fins de consultation en janvier 2001 puis amendé par le groupe à la suite des commentaires reçus. Le Comité diffuse actuellement dans le monde sa version révisée, dans l'espoir que le dispositif CC présenté serve de référence aux autorités de contrôle pour élaborer des pratiques nationales et aux banques pour concevoir leurs propres programmes. Il convient de préciser que les pratiques prudentielles de certaines juridictions atteignent ou dépassent déjà l'objectif de ce document et n'auront peut-être pas lieu d'être modifiées.

3. La connaissance de la clientèle est très étroitement associée à la lutte contre le blanchiment, qui est essentiellement du ressort du Groupe d'action financière sur le blanchiment de capitaux (GAFI)². Le Comité, qui n'entend pas reprendre les travaux du GAFI, œuvre dans une perspective prudentielle plus large. De saines politiques et procédures CC jouent un rôle majeur pour préserver la sûreté et la solidité des banques ainsi que l'intégrité des systèmes bancaires. Le Comité et le Groupe offshore des autorités de contrôle bancaire demeurent résolument favorables à l'adoption et la mise en œuvre des recommandations du GAFI, notamment celles qui concernent les banques, et désirent que les normes contenues dans ce document soient compatibles avec les recommandations du GAFI. Le Comité et le Groupe offshore envisageront également d'adopter des critères plus rigoureux qui seraient introduits par le GAFI, à la suite de la révision qu'il effectue actuellement de ses 40 recommandations. C'est la raison pour laquelle le Groupe de travail maintiendra ses contacts étroits avec le GAFI au fur et à mesure que celui-ci poursuivra sa réflexion.

4. L'approche CC du Comité de Bâle s'inscrit, au-delà de la lutte contre le blanchiment, dans une perspective prudentielle plus vaste. De saines procédures à cet égard doivent être considérées comme un aspect essentiel d'une gestion efficace des risques bancaires. Les mesures de protection dépassent le cadre d'une simple opération d'ouverture et de tenue de compte; elles exigent de la part des banques la mise au point d'une politique d'acceptation de la clientèle et d'un programme d'identification à plusieurs niveaux impliquant un devoir de diligence plus rigoureux à l'égard des comptes à hauts risques et une surveillance vigilante des activités suspectes.

5. L'intérêt du Comité de Bâle pour des normes CC saines est lié à son souci d'intégrité du marché et a été avivé par les pertes, directes et indirectes, encourues par des banques à cause de

¹ Groupe de travail conjoint comprenant des membres du Comité de Bâle et du Groupe offshore des autorités de contrôle bancaire.

² Organisme intergouvernemental qui a pour objectif de concevoir et de promouvoir des stratégies nationales et internationales de lutte contre le blanchiment de capitaux. Le GAFI compte 29 pays membres et deux organisations régionales. Il travaille en étroite coopération avec d'autres instances internationales actives dans ce domaine, telles que le Bureau des Nations Unies du contrôle des drogues et de la prévention des crimes, le Conseil de l'Europe, le Groupe Asie-Pacifique sur le blanchiment d'argent et la Caribbean Financial Action Task Force. Le GAFI définit le blanchiment de capitaux comme le processus consistant à retenir les produits d'origine criminelle pour en masquer l'origine illégale.

leur manque de diligence dans l'application de procédures appropriées. Ces pertes auraient probablement pu être évitées et auraient nettement moins affecté la réputation des établissements si ceux-ci avaient disposé de programmes CC efficaces.

6. Le présent document conforte les principes déjà définis dans des rapports antérieurs du Comité, en fournissant des indications plus précises sur les éléments essentiels des normes CC et sur leur mise en œuvre. À cet effet, le Groupe de travail s'est inspiré des pratiques suivies dans les pays membres et a pris en compte l'évolution dans le domaine prudentiel. Les éléments essentiels présentés dans ce document constituent des recommandations de normes minimales applicables par les banques à l'échelle mondiale. Ces normes pourront être complétées au besoin et/ou renforcées par des mesures complémentaires adaptées aux risques encourus par des établissements particuliers ou par le système bancaire de tel ou tel pays. Ainsi, un surcroît de diligence est requis à l'égard des comptes à hauts risques ou de la part des banques qui cherchent précisément à attirer une clientèle à patrimoine élevé. Plusieurs parties de ce document comportent des recommandations de normes de diligence plus strictes destinées, le cas échéant, aux domaines à hauts risques des banques.

7. Les banques ne sont pas les seules à avoir besoin de normes de diligence rigoureuses à l'égard de la clientèle. Le Comité est convaincu que des recommandations du même ordre doivent être élaborées pour tous les établissements financiers non bancaires et intermédiaires offrant des services financiers tels que juristes et comptables.

II. Importance des normes CC pour les autorités de contrôle et les banques

8. Le GAFI ainsi que d'autres instances internationales ont œuvré intensément sur les questions CC, et les 40 recommandations du GAFI sur la lutte contre le blanchiment de capitaux sont reconnues et appliquées dans le monde entier³. L'objet du présent document n'est donc pas de reprendre ces travaux.

9. Dans le même temps, de saines procédures CC présentent une importance particulière pour la sécurité et la solidité des banques dans la mesure où:

- elles contribuent à préserver la réputation des banques et l'intégrité des systèmes bancaires, en réduisant la probabilité que les établissements ne deviennent instruments ou victimes de criminalité financière et ne subissent de graves préjudices résultant d'une atteinte à leur réputation;
- elles constituent un élément essentiel d'une saine gestion des risques (par exemple, en permettant l'identification, la limitation et le contrôle des expositions en regard d'actifs et de passifs, y compris les actifs gérés).

10. L'inadéquation ou l'absence de normes CC peut exposer les banques à des risques sérieux liés à sa clientèle et à ses contreparties, notamment **risque d'atteinte à la réputation, risque opérationnel, risque juridique et risque de concentration**. Il est intéressant de noter que tous ces risques, bien qu'interdépendants, peuvent entraîner individuellement des coûts financiers substantiels pour les banques (sous la forme, par exemple, de retraits de fonds par des déposants, de ruptures de facilités interbancaires, d'actions contre l'établissement, de frais d'enquête, de saisies et gels d'actifs ainsi que de pertes sur prêts) et nécessiter, de la part des dirigeants, beaucoup de temps et d'énergie pour résoudre les problèmes qui se posent.

11. Le **risque d'atteinte à la réputation** constitue une lourde menace pour les banques, étant donné que la nature de leurs activités nécessite le maintien de la confiance des déposants, des créanciers et du marché en général. Ce risque se définit comme l'éventualité qu'une publicité défavorable, justifiée ou non, concernant des pratiques et connexions d'une banque n'entraîne une perte de confiance dans l'intégrité de l'établissement. Les banques sont particulièrement vulnérables à ce type de risque, car elles peuvent facilement devenir l'instrument ou la cible d'activités illégales de

³ Recommandations 10 à 19, Annexe 2.

leurs clients. Elles doivent se protéger en exerçant une vigilance constante grâce à un programme CC efficace. Les actifs gérés ou détenus en fiducie peuvent poser des risques spécifiques d'atteinte à la réputation.

12. Le **risque opérationnel** peut se définir comme le risque de pertes directes ou indirectes résultant d'une inadéquation ou d'une défaillance attribuable à des procédures, personnes, systèmes internes ou à des événements extérieurs. Dans le contexte CC, la plupart des cas de risque opérationnel sont liés à des lacunes dans la mise en œuvre des programmes des banques, à l'inefficacité des procédures de contrôle et à des manquements au devoir de diligence. Si le public a l'impression qu'une banque n'est pas capable de gérer efficacement son risque opérationnel, les affaires de celle-ci peuvent en être perturbées ou compromises.

13. Le **risque juridique** réside dans la possibilité que des procès, des jugements défavorables ou l'impossibilité d'exécution de contrats perturbent ou compromettent les opérations ou la situation d'un établissement. Des banques peuvent faire l'objet de poursuites du fait de la non-observation de normes CC obligatoires ou de manquement au devoir de diligence. Elles peuvent alors encourir des amendes, responsabilités pénales ou sanctions spéciales imposées par les autorités de contrôle. D'ailleurs, le fait d'être impliqué dans un procès peut avoir pour une banque des répercussions financières bien plus coûteuses que les simples frais de procédure. Les banques ne seront pas en mesure de se protéger efficacement de tels risques juridiques si elles n'assument pas leur devoir de diligence dans l'identification de la clientèle et la connaissance de leurs activités.

14. Les préoccupations prudentielles relatives au **risque de concentration** concernent essentiellement l'actif du bilan. En règle générale, non seulement les autorités de contrôle exigent des banques qu'elles disposent de systèmes d'information permettant de déceler les concentrations de crédits, mais, la plupart du temps, elles fixent aussi des limites prudentielles à leurs expositions envers des emprunteurs individuels ou groupes d'emprunteurs liés. Sans connaissance précise de ses clients et des relations qui existent au sein de sa clientèle, il sera impossible à une banque de mesurer son risque de concentration, surtout en présence de contreparties liées ou de prêts apparentés.

15. Au passif, le risque de concentration est étroitement lié au risque de financement, notamment le risque de retrait anticipé et soudain de fonds de la part de gros déposants, qui peut avoir des conséquences néfastes pour la liquidité de la banque. Le risque de financement est sans doute plus élevé pour les banques de petite taille et les établissements relativement peu actifs sur les marchés de gros. Pour analyser les concentrations de dépôts, les banques doivent connaître les caractéristiques de leurs déposants, c'est-à-dire non seulement leur identité mais aussi les interactions éventuelles avec d'autres déposants. Il est essentiel que les gestionnaires de passif des petites banques connaissent les gros déposants et entretiennent des relations étroites avec eux; sinon, ils courent le risque de perdre leurs fonds à des moments critiques.

16. Il arrive fréquemment que des clients aient plusieurs comptes auprès du même établissement, mais dans des pays différents. Pour gérer efficacement le risque d'atteinte à la réputation, le risque de non-respect des règles et le risque juridique inhérents à ces comptes, les banques devraient être capables d'agréger et de surveiller les soldes et transactions importants de ces comptes sur une base consolidée à l'échelle mondiale, que les actifs soient au bilan, gérés au hors-bilan ou détenus en fiducie.

17. Le Comité de Bâle comme le Groupe offshore des autorités de contrôle bancaire sont pleinement convaincus que des pratiques CC efficaces devraient faire partie intégrante des systèmes de gestion des risques et de contrôles internes dans toutes les banques. Il incombe aux responsables prudentiels nationaux de s'assurer que les établissements disposent de normes minimales et de contrôles internes leur procurant une connaissance adéquate de leur clientèle. Les codes de conduite à adhésion volontaire élaborés par les organisations ou associations professionnelles peuvent être très utiles pour étayer les recommandations réglementaires, par les conseils pratiques qu'ils donnent aux banques sur des questions opérationnelles⁴, mais ne sauraient toutefois s'y substituer.

⁴ C'est le cas, par exemple, des *Global anti-money-laundering guidelines for Private Banking* (ou Principes Wolfsberg), publiés en octobre 2000 par douze grandes banques ayant d'importantes activités de banque privée.

III. Éléments essentiels des normes CC

18. Le Comité de Bâle a publié des recommandations CC dans trois documents, qui reflètent l'évolution dans le temps de la pensée prudentielle. Le premier, *Prévention de l'utilisation du système bancaire pour le blanchiment de fonds d'origine criminelle* (1988), expose les principes éthiques de base et encourage les banques à mettre en place des procédures efficaces pour identifier la clientèle, refuser les transactions douteuses et coopérer avec les instances chargées de l'application des lois. Le deuxième, *Principes fondamentaux pour un contrôle bancaire efficace* (1997), procède à une analyse plus large des contrôles internes; il précise que les banques devraient disposer de politiques, pratiques et procédures appropriées - notamment des règles CC rigoureuses - et que les autorités de contrôle devraient encourager l'adoption des recommandations correspondantes du GAFI. Celles-ci portent sur l'identification des clients et la conservation des documents, une diligence accrue des institutions financières pour détecter et notifier les transactions douteuses ainsi que sur les mesures à appliquer à l'égard des pays où les dispositions contre le blanchiment de capitaux sont inadéquates. La *Méthodologie des Principes fondamentaux* (1999) complète le document de 1997 en énumérant plusieurs autres critères essentiels additionnels (les passages concernés des *Principes fondamentaux* et de la *Méthodologie* sont reproduits dans l'Annexe 1).

19. Toutes les banques devraient être tenues de «disposer de politiques, pratiques et procédures de nature à promouvoir un haut degré d'éthique et de professionnalisme et à empêcher qu'elles ne soient utilisées, intentionnellement ou non, dans le cadre d'activités criminelles»⁵. Lors de l'élaboration de leurs programmes CC, elles devraient prendre en compte certains éléments essentiels dès le stade de la gestion des risques et des procédures de contrôle: 1) politique d'acceptation des nouveaux clients; 2) identification de la clientèle; 3) surveillance continue des comptes à hauts risques; 4) gestion des risques. Les banques devraient non seulement déterminer l'identité de leurs clients mais surveiller aussi les mouvements de comptes pour déceler les transactions atypiques ou inhabituelles pour un client précis ou une catégorie de compte. La connaissance de la clientèle devrait constituer un élément clé de la gestion des risques et des procédures de contrôle des banques et être régulièrement complétée par des vérifications du respect des règles et un audit interne. Indépendamment de cela, l'intensité des programmes CC devrait être adaptée au degré de risque.

1. Politique d'acceptation des nouveaux clients

20. Les banques devraient définir des politiques et procédures claires d'acceptation des nouveaux clients comprenant notamment la description des types de clientèle susceptibles de représenter pour elles un risque supérieur à la moyenne. Pour cela, elles devraient prendre en compte des facteurs tels que les antécédents de leurs clients, leur pays d'origine, le fait qu'il s'agit de personnages publics ou en vue, les liens entre comptes, leurs activités professionnelles ainsi que d'autres indicateurs de risque. Ces politiques et procédures des banques devraient être graduées, c'est-à-dire qu'elles devraient requérir un renforcement du devoir de diligence vis-à-vis de la clientèle à hauts risques; ainsi, une personne exerçant une activité rémunérée présentant un faible solde pourrait se voir appliquer les exigences les plus élémentaires en matière d'ouverture de compte. Il convient de veiller, cependant, à ce que la politique d'acceptation des nouveaux clients ne soit pas à ce point restrictive qu'elle empêche le grand public, en particulier les personnes en situation financière ou sociale précaire, d'accéder aux services bancaires. En revanche, un devoir de diligence très rigoureux serait indispensable envers une personne ayant une fortune élevée d'origine incertaine. La décision d'ouvrir des relations d'affaires avec des clients à hauts risques, tels que des personnes politiquement exposées (voir 2.2.3), devrait être prise exclusivement au niveau de la direction générale.

⁵ *Méthodologie des Principes fondamentaux*, Critère essentiel n° 1.

2. Identification de la clientèle

21. L'identification de la clientèle est un élément clé des normes CC. Aux fins du présent document, on désigne par le terme «client»:

- toute personne ou entité titulaire d'un compte auprès de la banque ou au nom de laquelle un compte est ouvert (bénéficiaire effectif du compte);
- les bénéficiaires de transactions effectuées par des intermédiaires professionnels;
- toute personne ou entité associée à une transaction financière susceptible d'entraîner, pour la banque, un risque important d'atteinte à la réputation ou d'autre nature.

22. Les banques devraient prévoir une procédure systématique d'identification des nouveaux clients et ne pas ouvrir de relations d'affaires avec un client tant que son identité n'est pas dûment vérifiée.

23. Les banques devraient disposer de «politiques explicitées et appliquées pour identifier les clients et leurs mandataires»⁶. Pour vérifier l'identité des clients, les meilleurs documents sont ceux qui sont le plus difficile à obtenir illicitement et à contrefaire. Une attention particulière devrait être consacrée aux clients non résidents, et une banque ne devrait en aucun cas renoncer aux procédures d'identification pour la simple raison que le nouveau client n'est pas en mesure d'être présent en personne à un entretien. Les banques devraient toujours se demander pourquoi le client a choisi d'ouvrir un compte dans une juridiction étrangère.

24. La procédure d'identification intervient normalement lors de l'établissement de la relation d'affaires. Pour s'assurer que les données qu'elles détiennent sont d'actualité, les banques doivent les revoir régulièrement, par exemple à l'occasion d'une grosse transaction, d'une modification substantielle des normes de documentation sur la clientèle ou d'un changement important dans le mode de gestion du compte⁷. Toutefois, si une banque réalise à un moment donné qu'elle manque d'informations au sujet d'un client existant, elle devra prendre des mesures pour obtenir le plus tôt possible tous les renseignements nécessaires.

25. Les établissements offrant des services de banque privée, particulièrement exposés au risque d'atteinte à la réputation, devraient renforcer leur devoir de diligence sur ces opérations. Des comptes de banque privée, qui impliquent par nature une grande part de confidentialité, peuvent être ouverts au nom d'un individu, d'une entreprise commerciale, d'une société fiduciaire, d'un intermédiaire ou d'une entreprise d'investissement personnalisée. Dans tous les cas, un risque d'atteinte à la réputation peut apparaître si la banque ne suit pas avec diligence les procédures CC établies. Tout nouveau client ou compte devrait être approuvé par au moins une personne, de niveau hiérarchique suffisamment élevé, autre que le chargé de relation pour les activités de banque privée. Même si des mesures spécifiques sont prises à l'intérieur de la banque pour préserver la confidentialité des clients et de leurs transactions dans ce domaine, les établissements doivent veiller à ce qu'il soit toujours possible de soumettre ces clients et leurs opérations à un examen et une surveillance au moins aussi rigoureux, sous la forme, par exemple, d'une inspection des responsables conformité et des auditeurs.

26. Les banques devraient élaborer «des règles claires [précisant] quelles sont les données à conserver sur l'identification de la clientèle et les transactions individuelles et sur quelle durée»⁸. De telles pratiques sont essentielles pour qu'un établissement puisse surveiller sa relation avec le client, comprendre ses activités courantes et, si nécessaire, fournir des preuves en cas de différend, d'action judiciaire ou d'enquête financière pouvant conduire à des poursuites pénales. Pour entamer la procédure d'identification et en exploiter les résultats, les banques devraient se procurer des pièces d'identité du client et en conserver des copies pendant au moins cinq ans après la clôture du compte. Elles devraient également garder, sur la même période, tous les enregistrements des transactions financières à compter de leur réalisation.

⁶ *Méthodologie des Principes fondamentaux*, Critère essentiel n° 2.

⁷ L'application de nouvelles normes CC aux comptes existants est actuellement soumise à l'appréciation du GAFI.

⁸ *Méthodologie des Principes fondamentaux*, Critère essentiel n° 2.

2.1 Exigences générales d'identification

27. Les banques doivent obtenir toutes les informations nécessaires pour établir, à leur entière satisfaction, l'identité de chaque nouveau client ainsi que l'objet et la finalité de la relation. L'ampleur et la nature des données dépendent de la qualité du candidat (particulier, entreprise, etc.) et du solde prévu sur le compte. Les autorités de contrôle nationales sont invitées à fournir des recommandations pour aider les banques à mettre au point leurs procédures d'identification. Le Groupe de travail se propose de définir les éléments essentiels des exigences à cet égard.

28. Quand, après l'ouverture d'un compte, apparaissent des problèmes de vérification insolubles, la banque devrait fermer le compte et restituer le solde⁹.

29. Si une banque peut être assez confiante lorsque, pour l'ouverture d'un compte, elle reçoit des fonds d'un autre établissement soumis aux mêmes normes CC, elle devrait cependant envisager la possibilité que le gestionnaire précédent ait demandé la fermeture du compte par crainte d'activités douteuses. Un client a naturellement le droit de transférer un compte d'un établissement à un autre. Toutefois, si une banque a la moindre raison de penser qu'un candidat s'est vu exclure des services bancaires, elle devrait renforcer les procédures CC à son égard.

30. Une banque ne devrait jamais accepter d'ouvrir un compte ou de maintenir des relations d'affaires avec un client qui exige l'anonymat ou se présente sous un faux nom. Les comptes à numéro confidentiel¹⁰ ne devraient pas, non plus, servir à protéger l'anonymat, mais être soumis aux procédures CC normales, même si les vérifications sont effectuées par un personnel spécial. Si un compte à numéro peut offrir une plus grande confidentialité à son titulaire, l'identité de celui-ci doit cependant être connue d'un nombre d'employés suffisant à l'exercice adéquat du devoir de diligence. En aucun cas, ces comptes ne sauraient être utilisés pour dissimuler l'identité du client à la fonction conformité de l'établissement ou aux autorités prudentielles.

2.2 Aspects particuliers de l'identification

31. Plusieurs aspects particuliers doivent être précisés. Certains sont actuellement examinés par le GAFI dans le cadre de la révision générale de ses 40 recommandations, et le Groupe de travail reconnaît la nécessité d'une harmonisation avec ses travaux.

2.2.1 Comptes de fiducie et de mandataire

32. Les comptes de fiducie et de mandataire peuvent servir à contourner les procédures d'identification de la clientèle. S'il peut être justifié, dans certaines circonstances, d'offrir un niveau de sécurité supplémentaire pour préserver la confidentialité d'une activité légitime de banque privée, il est essentiel que la banque comprenne la véritable nature de la relation. Elle devrait établir si un client se fait passer pour un autre, s'il sert de «couverture» ou s'il agit au nom d'un tiers en qualité d'intermédiaire, tel que fidéicommiss. En pareil cas, il est nécessaire qu'elle reçoive, préalablement à l'ouverture du compte, des justificatifs de l'identité de tous les intermédiaires et des personnes au nom desquelles ils agissent ainsi que des précisions concernant la nature de la fiducie ou de tout autre arrangement conclu. En présence d'une fiducie, l'identification porte également sur les fidéicommiss, fiduciaires/constituants et bénéficiaires¹¹.

2.2.2 Personnes morales

33. Les banques doivent exercer leur vigilance pour éviter que des particuliers n'aient recours à des personnes morales pour disposer en fait de comptes anonymes. Dans le cas de structures (comme les International Business Companies - IBC) détenant des actifs individuels, l'identification du

⁹ Sous réserve des réglementations nationales concernant le traitement des opérations suspectes.

¹⁰ Le nom du bénéficiaire d'un tel compte est connu de la banque, mais remplacé par un numéro ou code dans la documentation ultérieure.

¹¹ Dans la mesure du possible, les bénéficiaires devraient être identifiés lorsqu'ils sont définis. Cela peut ne pas être possible d'emblée. C'est le cas, par exemple, s'il s'agit d'enfants à naître ou si le bénéfice est subordonné à la réalisation d'événements déterminés. En outre, les bénéficiaires définis comme groupe (par exemple participants à un fonds de pension) peuvent à juste titre être traités à l'instar des comptes collectifs (paragraphe 38-39).

client ou bénéficiaire peut être difficile. Une banque devrait comprendre la structure de la société, déterminer la provenance des fonds et identifier leurs bénéficiaires ainsi que les personnes qui contrôlent ces fonds.

34. Une banque doit être spécialement vigilante lors de l'ouverture de relations avec des sociétés dont le capital est constitué d'actions au porteur ou détenu par des mandataires. Elle doit obtenir des justificatifs établissant de manière satisfaisante l'identité des bénéficiaires. Sa vigilance doit être accrue dans le cas de sociétés dont une part importante du capital se présente sous forme d'actions au porteur, celles-ci pouvant changer de mains à son insu. Il incombe aux banques de mettre en place des procédures satisfaisantes de contrôle de l'identité des principaux bénéficiaires, au besoin en immobilisant les actions, par exemple en les conservant en dépôt.

2.2.3 *Clientèle recommandée*

35. Les procédures d'identification peuvent prendre beaucoup de temps et les banques désirent naturellement éviter les désagréments pour leurs nouveaux clients. Aussi, dans certains pays, il est courant qu'elles s'en remettent aux procédures menées par d'autres établissements ou des intermédiaires lorsque ceux-ci leur adressent un client. Dans ce cas, elles risquent d'accorder une confiance excessive aux procédures CC que ces tiers sont censés avoir réalisées. Se fonder sur elles, quelle que soit la réputation de l'intermédiaire, ne dispense pas les banques de connaître leur clientèle et ses activités, responsabilité qui leur incombe en dernière instance. Les banques devraient notamment ne pas faire confiance à des intermédiaires soumis à des normes inférieures à leurs propres procédures CC ou qui refusent de communiquer les informations obtenues dans l'exercice de leur devoir de diligence.

36. Le Comité de Bâle recommande à une banque ayant recours à de tels intermédiaires d'évaluer soigneusement leur compétence et leur honorabilité et de vérifier qu'ils exercent le devoir de diligence exigé par les normes exposées dans le présent document. La responsabilité finale en matière de CC incombe toujours à la banque, qui devrait utiliser les critères suivants pour déterminer la fiabilité d'un tiers¹²:

- il doit respecter les pratiques minimales au titre du devoir de diligence exposées dans ce document;
- ses procédures liées au devoir de diligence doivent être aussi rigoureuses que celles que la banque aurait appliquées elle-même à l'égard de sa clientèle;
- la banque doit s'assurer de la fiabilité des systèmes qu'il a mis en place pour vérifier l'identité des clients;
- la banque doit avoir obtenu de lui l'autorisation de vérifier comment il s'acquitte à chaque stade de son devoir de diligence;
- il doit, sans délai, soumettre à la banque les informations de toute nature concernant l'identité des clients et celle-ci doit les examiner soigneusement. Ces informations doivent être tenues à la disposition de l'autorité prudentielle et de l'organisme de renseignement financier ou autorité exerçant des compétences équivalentes, lorsque la loi leur confère ce pouvoir.

En outre, les banques devraient effectuer des examens périodiques pour s'assurer que l'intermédiaire auquel elles font confiance remplit toujours les critères exposés ci-dessus.

2.2.4 *Comptes clients ouverts par des intermédiaires professionnels*

37. Lorsqu'une banque sait ou a des raisons de penser qu'un intermédiaire professionnel a ouvert un compte au bénéfice d'un client unique, celui-ci doit être identifié.

38. Les banques disposent souvent de comptes collectifs, soit gérés par des intermédiaires professionnels agissant au nom d'entités telles que fonds communs de placement, fonds de pension et fonds de trésorerie, soit contenant des sommes en dépôt ou sous séquestre gérées par des juristes

¹² Le GAFI examine actuellement s'il convient d'agréer de tels intermédiaires.

ou courtiers en faveur de divers clients. Si les sommes détenues par l'intermédiaire ne sont pas fusionnées mais réparties en sous-comptes correspondant aux différents bénéficiaires, ceux-ci doivent être tous identifiés.

39. Lorsque les sommes sont fusionnées, leur bénéficiaire devrait être transparent pour la banque. Dans certains cas, il n'est peut-être pas nécessaire que la banque aille en amont de l'intermédiaire, par exemple quand celui-ci est soumis aux mêmes réglementations et procédures relatives au contrôle prudentiel et au blanchiment de capitaux, notamment en ce qui concerne le devoir de diligence. Les recommandations des autorités prudentielles nationales devraient clairement préciser ces cas. Les banques devraient accepter de tels comptes uniquement si elles peuvent établir que l'intermédiaire a effectué un processus CC adéquat et qu'il dispose des systèmes et contrôles nécessaires pour affecter correctement les actifs en compte à leurs propriétaires respectifs. Pour évaluer la façon dont l'intermédiaire s'acquitte de son devoir de diligence, la banque devrait avoir recours aux critères énoncés au paragraphe 36.

40. Lorsque l'intermédiaire n'est pas habilité à fournir à la banque les informations nécessaires sur les bénéficiaires (par exemple, juristes tenus au secret professionnel¹³) ou lorsqu'il n'est pas assujéti à des normes de diligence équivalentes à celles énoncées ici ou à celles d'une législation antiblanchiment rigoureuse), la banque ne devrait pas lui permettre d'ouvrir un compte.

2.2.5 Personnes politiquement exposées (PPE)

41. Entretenir des relations d'affaires avec les détenteurs de postes publics élevés et des personnes ou sociétés qui leur sont clairement liées peut exposer la banque à un risque d'atteinte à la réputation et/ou un risque juridique non négligeables. Les personnes politiquement exposées exercent ou ont exercé d'importantes fonctions publiques: chefs d'État ou de gouvernement, figures politiques, hauts fonctionnaires de l'administration, de la magistrature ou de l'armée, cadres dirigeants de sociétés publiques et responsables de grand parti politique, par exemple. On ne peut exclure, notamment dans les pays où la corruption est répandue, que ces personnes abusent de leur pouvoir officiel pour obtenir un enrichissement personnel par des voies illicites (pots-de-vin, détournement de fonds, etc.).

42. Accepter et gérer les fonds de PPE corrompues entache gravement la réputation de l'établissement et peut ébranler la confiance du public dans les normes éthiques de tout centre financier, étant donné que les affaires de cette nature reçoivent normalement une importante couverture médiatique et suscitent une vive réaction politique, même s'il est souvent difficile de prouver l'origine illicite des actifs. En outre, la banque peut faire l'objet, de la part des autorités policières ou judiciaires, de demandes d'informations et mesures de saisie coûteuses (pouvant aller jusqu'à des procédures internationales d'assistance mutuelle en matière pénale), voire être appelée en dommages-intérêts par l'État lésé ou les victimes d'un régime. Dans certaines circonstances, la banque et/ou ses responsables et employés peuvent être eux-mêmes exposés à des accusations de blanchiment s'ils savaient, ou auraient dû savoir, que les fonds provenaient d'activités criminelles (corruption, par exemple).

43. Certains pays viennent d'amender, ou modifient, leur législation et leur réglementation de façon à criminaliser la corruption active de fonctionnaires et agents publics étrangers, conformément à la convention internationale sur ce sujet¹⁴. Dans ces juridictions, la corruption d'agents étrangers est qualifiée d'acte de blanchiment et tombe ainsi sous le coup de toutes les lois et réglementations antiblanchiment (par exemple, déclaration des transactions douteuses, interdiction d'informer le client, gel interne des fonds, etc.). Toutefois, même en l'absence d'une telle base légale explicite en droit pénal, il est évidemment peu souhaitable pour une banque, contraire à l'éthique - comme au critère de compétence et d'honorabilité dans la conduite des opérations -, d'accepter ou d'entretenir des relations d'affaires lorsqu'elle sait, ou a toutes les raisons de penser, que les fonds proviennent d'actes de corruption ou d'un détournement de fonds publics. Une banque envisageant d'établir une

¹³ Le GAFI procède actuellement à un examen des procédures CC régissant les comptes ouverts par des juristes au nom de leurs clients.

¹⁴ OCDE: Convention sur la lutte contre la corruption d'agents publics étrangers dans les transactions commerciales internationales, adoptée par la Conférence de négociations le 21 novembre 1997.

relation d'affaires avec une personne qu'elle soupçonne être politiquement exposée doit l'identifier avec précision, de même que les particuliers et sociétés qui lui sont manifestement liés.

44. Les banques devraient obtenir d'un nouveau client suffisamment de renseignements et vérifier les sources d'information publique afin d'établir s'il s'agit d'une PPE. Dans ce cas, elles devraient se renseigner sur l'origine de ses fonds avant de l'admettre, décision qui relève de la haute direction.

2.2.6. *Clients à distance*

45. De plus en plus, il est demandé aux banques d'ouvrir un compte au nom de clients qui ne se présentent pas en personne pour un entretien. Courante dans le cas de la clientèle non résidente, cette pratique s'est fortement développée avec l'expansion récente de la banque postale, téléphonique et électronique. Les banques devraient appliquer à ces clients des procédures d'identification et des normes de surveillance permanente tout aussi efficaces qu'avec les autres. La possibilité d'une vérification indépendante par un tiers de réputation confirmée a été évoquée à cet égard. L'ensemble de cette question est examiné par le GAFI ainsi que dans le contexte de la modification de la Directive CEE de 1991.

46. L'exemple typique est celui du client qui souhaite effectuer des opérations bancaires par Internet ou une technologie similaire. La banque électronique offre aujourd'hui une large gamme de produits et services accessibles par les réseaux de télécommunications; sa nature impersonnelle et transfrontière, combinée à la vitesse des transactions, rend nécessairement difficile l'identification des clients et la vérification. Les autorités de contrôle attendent des banques, au minimum, qu'elles anticipent les différents risques suscités par les technologies émergentes et mettent au point des procédures d'identification de la clientèle les prenant dûment en compte¹⁵.

47. Bien que la documentation à fournir soit la même pour tous, les banques ont plus de difficulté à vérifier que les informations correspondent au client en l'absence de contact physique. Le problème de la vérification se pose avec encore plus d'acuité dans le cas des relations par voies téléphonique et informatique.

48. Pour accepter de nouveaux clients à distance, les banques devraient:

- leur appliquer des procédures d'identification tout aussi efficaces que pour les clients se présentant à un entretien;
- prendre des mesures spécifiques et adéquates pour limiter ce risque accru, notamment:
 - authentification des documents présentés;
 - demande de documents supplémentaires;
 - contact indépendant avec le client;
 - intermédiation d'un tiers, sous réserve des critères énoncés au paragraphe 36; ou
 - exigence d'un premier paiement par l'intermédiaire d'un compte ouvert au nom du client auprès d'un établissement soumis à des normes de diligence semblables.

2.2.7 *Banques correspondantes*

49. Une banque correspondante offre des services bancaires à une autre. Utilisé dans le monde entier, ce système permet aux banques d'exercer des activités et de fournir des services de manière indirecte. Certains comptes, méritant une attention particulière, proposent des services dans des juridictions où la banque n'est pas physiquement présente. Une banque qui n'appliquerait pas à ces comptes un devoir de diligence adéquat s'exposerait aux risques recensés dans le rapport et pourrait détenir et/ou transmettre des fonds liés à une activité illégale telle que corruption ou fraude.

50. Les banques devraient rassembler suffisamment d'informations sur leurs correspondants pour bien comprendre la nature de leurs activités. Elles devraient notamment se renseigner sur les

¹⁵ Le Groupe sur la banque électronique du Comité de Bâle a publié, en mai 2001, un document sur les principes de gestion des risques dans la banque électronique.

aspects suivants: organes de direction; principales activités et lieu d'implantation; efforts de prévention et de détection du blanchiment; finalité du compte; identité de tous les utilisateurs des services du correspondant; état de la réglementation et du contrôle bancaires dans le pays. Une banque ne devrait établir de relations de correspondant qu'avec des établissements étrangers efficacement contrôlés par les autorités compétentes. De leur côté, ceux-ci devraient disposer de politiques CC efficaces, en particulier pour l'acceptation de nouveaux clients.

51. Les banques devraient notamment refuser d'établir ou de conserver des relations de correspondant avec un établissement soit enregistré dans une juridiction où il n'est pas présent physiquement, soit non apparenté à un groupe financier réglementé (cas des «coquilles vides» ou façades comptables). Elles devraient se montrer particulièrement vigilantes lorsqu'elles maintiennent des relations avec des établissements situés dans des juridictions ayant des normes CC insuffisantes ou ayant été classées «non coopératives» dans la lutte contre le blanchiment. Elles devraient s'assurer que les établissements à qui elles offrent des services de correspondant appliquent leur devoir de diligence conformément aux normes présentées dans ce document et renforcer leurs procédures pour les transactions transitant par les comptes de correspondant.

52. Les banques devraient être particulièrement attentives au risque d'utilisation directe par des tiers de ces comptes de correspondant (sur comptes de passage, par exemple). De tels dispositifs appellent, en général, les mêmes réserves que la clientèle recommandée et devraient être traités conformément aux critères exposés au paragraphe 36.

3. Surveillance continue des comptes et transactions

53. Une surveillance continue est essentielle à l'efficacité des procédures CC. Le contrôle et la réduction des risques ne peuvent être efficaces que si les banques ont une bonne compréhension des activités normales et raisonnables sur les comptes de leur clientèle, de façon à identifier les transactions atypiques. Sans cette connaissance, elles manqueront vraisemblablement à leur devoir de déclaration des transactions suspectes aux autorités appropriées. La nature de la surveillance doit être fonction du degré de risque. Les banques devraient disposer de systèmes permettant, pour tous les comptes, de déceler les activités à caractère inhabituel ou suspect, en recourant, par exemple, à des limites par classe ou catégorie de comptes; une attention particulière devrait être accordée aux dépassements. Certains types d'opérations devraient éveiller les soupçons; c'est notamment le cas de celles qui ne semblent avoir aucune motivation économique ni commerciale ou qui portent sur des montants en liquide ne cadrant pas avec les transactions habituelles et concevables du client. Des mouvements de fonds démesurés par rapport au solde du compte peuvent être signe de blanchiment. Les banques trouveront très utile un catalogue d'activités suspectes, qui devrait figurer dans les procédures et/ou recommandations antiblanchiment d'une juridiction prudentielle.

54. Les comptes à hauts risques devraient faire l'objet d'une surveillance accrue. Chaque banque devrait les identifier grâce à une gamme d'indicateurs comportant des informations générales sur le client (pays d'origine et source des fonds, par exemple), le type de transaction et d'autres facteurs de risque. Pour ces comptes:

- les banques devraient s'assurer que les systèmes d'information de la direction sont aptes à fournir rapidement aux dirigeants et aux responsables conformité les renseignements permettant l'identification, l'analyse et la surveillance efficace de ces comptes. Divers rapports peuvent s'avérer nécessaires à cet effet: absence de documentation sur l'ouverture d'un compte, transactions inhabituelles et présentation consolidée des relations d'un client avec la banque;
- les cadres dirigeants chargés des activités de banque privée devraient connaître les détails personnels des clients à hauts risques et être attentifs à toute source d'information émanant de tiers; leurs grosses transactions devraient recevoir l'approbation d'un membre de la direction;
- les banques devraient se doter d'une politique claire ainsi que de lignes directrices, procédures et contrôles internes; elles devraient être extrêmement vigilantes dans leurs relations d'affaires avec les PPE et les personnalités ainsi qu'avec les particuliers et sociétés

qui leur sont clairement liés ou associés¹⁶. Étant donné que toutes les PPE ne peuvent pas être identifiées d'emblée et que ce statut peut s'acquérir, il importe de réexaminer régulièrement au moins les principaux clients.

4. Gestion des risques

55. L'efficacité des procédures CC repose sur le caractère adéquat de plusieurs éléments: surveillance par la direction, systèmes et contrôles, séparation des tâches, politiques de formation et autres. Le conseil d'administration devrait faire montre d'un engagement sans réserve à travers des procédures CC appropriées et leur application efficace. Les responsabilités devraient être explicitement définies au sein de la banque pour garantir que les politiques et procédures soient bien conduites et répondent, au minimum, aux pratiques prudentielles locales. Les modalités de déclaration des transactions suspectes devraient être clairement précisées par écrit et diffusées à l'ensemble du personnel. Des procédures internes devraient permettre, en outre, de déterminer si, dans le cadre de la législation correspondante, la banque est tenue d'en informer les autorités judiciaires et/ou prudentielles.

56. Une responsabilité majeure des fonctions audit interne et contrôle conformité consiste à vérifier le respect des politiques et procédures CC. En règle générale, le contrôle conformité devrait fournir une évaluation indépendante des politiques et procédures, couvrant également les aspects légaux et réglementaires. Il devrait être chargé, notamment, de la surveillance permanente par sondage de la conformité des prestations des agents et de l'analyse des comptes rendus de manquements, afin d'alerter la direction générale, ou le conseil d'administration s'il estime que celle-ci n'exerce pas pleinement ses responsabilités en matière de procédures CC.

57. L'audit interne a pour importante mission d'évaluer de manière indépendante la gestion et le contrôle des risques; il rend compte au comité d'audit du conseil d'administration ou à un organe de surveillance semblable en lui présentant des rapports périodiques sur le respect de la conformité aux politiques et procédures CC, sans omettre la formation du personnel. La direction devrait s'assurer que cette fonction dispose d'un personnel adéquat maîtrisant ces politiques et procédures. De plus, les auditeurs devraient faire preuve de diligence en veillant à ce que leurs conclusions et critiques soient suivies d'effet.

58. Chaque banque doit prévoir un programme permanent de formation préparant convenablement son personnel aux procédures CC. Le calendrier et le contenu des séances organisées pour les diverses unités devront être adaptés aux nécessités spécifiques de l'établissement. Les besoins de formation devraient être ajustés en fonction des participants: agents recrutés, employés en contact avec le public, responsables conformité, personnes chargées des nouveaux clients. Au moment de leur recrutement, les agents devraient être sensibilisés à l'importance des politiques CC et aux exigences fondamentales de la banque. Les employés en contact avec le public devraient apprendre à identifier les nouveaux clients, à faire preuve à tout moment de diligence dans le traitement des comptes clientèle et à déceler les activités suspectes. Des stages devraient rappeler périodiquement au personnel ses responsabilités et le tenir informé des derniers développements. Il est essentiel que chacun comprenne la nécessité des procédures CC et qu'elles soient appliquées de manière uniforme. Leur mise en œuvre efficace passe par une telle approche.

59. Dans de nombreux pays, les auditeurs externes ont également un rôle majeur à jouer en surveillant les contrôles et procédures internes des banques et en confirmant leur conformité aux pratiques prudentielles.

¹⁶ Il n'est pas réaliste d'attendre d'une banque qu'elle connaisse ou cherche à connaître toutes les relations familiales (surtout éloignées), politiques ou commerciales d'un client étranger. L'obligation de s'informer à l'apparition de soupçons dépend du volume des actifs ou de l'importance des mouvements de fonds, du contexte économique, de la réputation du pays concerné, de la solidité des explications données par le client, etc. Il convient toutefois de noter que les PPE (ou plus exactement leurs famille et amis) ne se présenteront pas forcément sous ce jour, mais plutôt comme des hommes d'affaires ordinaires (quoique aisés), sans révéler qu'elles doivent uniquement leur position élevée dans une entreprise légitime à leur relation privilégiée avec un haut responsable public.

IV. Rôle des autorités de contrôle

60. Il revient aux autorités de contrôle nationales d'élaborer, sur la base des normes internationales CC existantes, une approche prudentielle régissant les programmes des banques dans ce domaine. Les éléments essentiels exposés dans le présent document devraient constituer des recommandations claires permettant aux autorités de contrôle de concevoir ou d'améliorer l'approche prudentielle nationale.

61. Il incombe aux autorités de contrôle non seulement de formuler les éléments fondamentaux à respecter par les établissements bancaires, mais aussi de veiller à ce qu'ils observent constamment de saines procédures CC et des critères éthiques et professionnels. Elles devraient s'assurer qu'ils disposent de contrôles internes adéquats et se conforment aux recommandations prudentielles et réglementaires. Leur processus de surveillance devrait comporter un examen des politiques et procédures mais aussi des fichiers clients ainsi qu'une vérification des comptes par sondage. Elles devraient toujours avoir le droit de consulter l'ensemble de la documentation concernant les comptes ouverts dans leur juridiction, de même que toute étude effectuée par les banques pour déceler les transactions inhabituelles ou douteuses.

62. Les autorités de contrôle sont tenues de s'assurer que les établissements appliquent des normes CC élevées non seulement pour préserver leur sécurité et leur solidité, mais aussi pour protéger l'intégrité du système bancaire national¹⁷. Elles devraient indiquer clairement que, en cas de non-respect avéré des procédures internes et exigences réglementaires, elles prendront des mesures appropriées, sévères et publiques si les circonstances le justifient, à l'encontre des établissements et de leurs dirigeants. Elles devraient s'assurer, en outre, que les banques sont particulièrement attentives à toute transaction avec les juridictions où les normes ne sont pas considérées adéquates. Le GAFI et certaines autorités nationales ont établi une liste de pays et juridictions dont le cadre juridique et administratif est jugé non conforme aux normes internationales de lutte contre le blanchiment. Les banques devraient tenir compte de cette information dans leurs politiques et procédures CC.

V. Mise en œuvre des normes CC dans un contexte transfrontière

63. Toutes les autorités de contrôle devraient s'efforcer, dans toute la mesure du possible, d'élaborer et d'appliquer des normes CC nationales pleinement conformes aux normes internationales, de façon à éliminer les éventuels arbitrages réglementaires et à préserver l'intégrité des systèmes bancaires nationaux et internationaux. La mise en œuvre et l'évaluation de telles normes traduisent très concrètement la volonté des autorités de contrôle de coopérer avec leurs homologues et la capacité des banques à gérer les risques à l'échelle du groupe. Il s'agit là d'un enjeu de taille pour les banques comme pour les autorités prudentielles.

64. Les autorités de contrôle attendent des groupes bancaires qu'ils appliquent, pour leurs opérations domestiques et à l'étranger, des politiques et procédures CC obéissant à une norme minimale agréée. Pour être efficace, la surveillance des opérations bancaires internationales doit s'effectuer sur une base consolidée, le risque d'atteinte à la réputation comme les autres risques bancaires ne se confinant pas au territoire national. Les banques mères doivent transmettre leurs politiques et procédures à leurs succursales et filiales à l'étranger, y compris aux unités non bancaires (sociétés fiduciaires, par exemple), et disposer d'un processus régulier de vérification de la conformité à l'égard des normes CC des pays d'origine et d'accueil, pour assurer l'efficacité de leur programme à l'échelle mondiale. Ce processus sera soumis, lui aussi, à l'examen des auditeurs externes et autorités de contrôle. Il importe donc que la documentation CC soit bien archivée et tenue à leur disposition. Dans le cadre des tests de conformité, les autorités prudentielles et les auditeurs externes devraient, dans la plupart des cas, examiner les systèmes et contrôles et analyser par sondage les comptes clients ainsi que le suivi des transactions.

¹⁷ De nombreuses autorités de contrôle sont également tenues de déclarer toute transaction suspecte, inhabituelle ou illégale qu'elles ont décelée, par exemple à l'occasion d'examen sur place.

65. Même pour les plus petits établissements à l'étranger, un cadre supérieur devrait être chargé de s'assurer que tous les agents concernés sont formés à respecter des procédures CC conformes aux normes des pays d'origine et d'accueil et s'acquittent de cette tâche. Si cette responsabilité lui incombe directement, il devrait pouvoir s'appuyer, le cas échéant, sur les auditeurs internes et responsables conformité au niveau local et au siège.

66. En cas de différence entre les normes minimales CC des pays d'origine et d'accueil, les succursales et filiales à l'étranger devraient appliquer les plus exigeantes. D'une manière générale, aucun obstacle ne devrait s'opposer à ce qu'un établissement adopte des normes plus rigoureuses que le minimum local. Si, toutefois, le cadre juridique et réglementaire local (notamment en matière de secret bancaire) interdit l'application des normes plus élevées du pays d'origine, les autorités d'accueil devraient s'employer à le faire modifier. En attendant, les établissements locaux seraient tenus de respecter les normes du pays d'accueil, tout en indiquant clairement à leur siège/banque mère et à l'autorité de contrôle d'origine la nature de la différence de régime.

67. Comme les juridictions dressant de tels obstacles sont naturellement propices aux desseins criminels, les groupes bancaires devraient être conscients des gros risques d'atteinte à la réputation qu'elles présentent. Les banques mères devraient disposer d'une procédure pour examiner la vulnérabilité des diverses unités opérationnelles et adopter, au besoin, des protections supplémentaires. Au pire, les autorités prudentielles devraient envisager des contrôles additionnels sur les banques opérant dans ces juridictions, voire encourager leur départ.

68. Au cours des inspections sur place, les autorités d'origine ou auditeurs devraient pouvoir vérifier en toute liberté la conformité d'un établissement aux politiques et procédures CC, en examinant les fichiers clientèle et en vérifiant les comptes par sondage. Les autorités d'origine devraient avoir accès à l'information obtenue par sondage sur les comptes, dans la mesure où elle leur est nécessaire pour évaluer correctement la mise en œuvre des normes CC et les méthodes de gestion des risques; cet accès ne devrait pas être restreint par la législation locale sur le secret bancaire. Rien ne devrait s'opposer à la déclaration, sur une base consolidée, des concentrations en matière de dépôts et d'emprunts ou à la notification des fonds gérés pour compte de tiers, lorsque l'autorité d'origine l'exige. En outre, celle-ci peut, pour surveiller la concentration de dépôts ou le risque de financement en cas de retrait des dépôts, instituer des critères d'importance relative et des seuils en termes de bilan exigeant la communication de tout dépassement. Des précautions sont cependant indispensables pour que les informations sur un compte particulier soient utilisées exclusivement à des fins prudentielles légitimes et convenablement protégées par leur bénéficiaire. Une convention de coopération facilitant le partage bilatéral d'informations serait utile à cet égard¹⁸.

69. Dans certains cas, un conflit majeur peut opposer les politiques CC de la banque mère imposées par l'autorité d'origine et les dispositions permises dans l'un de ses établissements à l'étranger. Ainsi, la législation locale peut interdire les inspections sur place des responsables conformité/auditeurs internes de la banque mère ou des autorités d'origine, ou bien permettre à un client d'utiliser un faux nom ou de se dissimuler derrière des agents ou intermédiaires tenus au secret sur l'identité de leur client. Dans de tels cas, l'autorité d'origine devrait entrer en contact avec l'autorité d'accueil pour vérifier la réalité des obstacles juridiques et leur validité extraterritoriale. S'ils s'avèrent insurmontables et qu'aucune autre voie satisfaisante ne s'offre, l'autorité d'origine devrait préciser à son homologue que, à sa requête ou à l'initiative de la banque, l'établissement concerné pourrait être contraint de fermer. De toute façon, les dispositions régissant ces inspections sur place devraient prévoir une solution permettant à l'autorité d'origine d'effectuer une évaluation satisfaisante à son sens; il peut s'avérer utile de recourir à des conventions de coopération ou à des protocoles d'accord en définissant les modalités pratiques. Les autorités d'origine devraient disposer d'un accès à l'information aussi libre que possible et couvrant au minimum les politiques et procédures générales de la banque en matière de connaissance de la clientèle et de traitement des cas suspects.

¹⁸ Comité de Bâle sur le contrôle bancaire, *Essential elements of a statement of cooperation between banking supervisors* (mai 2001).

Annexe 1:

Extraits de *Méthodologie des Principes fondamentaux*

Principe 15: Les autorités de contrôle bancaire doivent s'assurer que les banques disposent de politiques, pratiques et procédures appropriées, notamment de critères stricts de connaissance de la clientèle, assurant un haut degré d'éthique et de professionnalisme dans le secteur financier et empêchant que la banque ne soit utilisée, intentionnellement ou non, dans le cadre d'activités criminelles.

Critères essentiels

1. L'autorité de contrôle s'assure que les banques disposent de politiques, pratiques et procédures de nature à promouvoir un haut degré d'éthique et de professionnalisme et à empêcher qu'elles ne soient utilisées, intentionnellement ou non, dans le cadre d'activités criminelles. Il s'agit notamment de prévenir et de repérer les actes délictueux ou frauduleux et d'informer les autorités compétentes des faits soupçonnés.
2. L'autorité de contrôle s'assure que les banques disposent de politiques explicites et appliquées pour identifier les clients et leurs mandataires dans le cadre de la lutte contre le blanchiment d'argent. Des règles claires précisent quelles sont les données à conserver sur l'identification de la clientèle et les transactions individuelles et sur quelle durée.
3. L'autorité de contrôle s'assure que les banques disposent de procédures formelles pour identifier les transactions potentiellement suspectes. Il peut s'agir d'autorisations supplémentaires pour les dépôts ou retraits en espèces importants ou de procédures spéciales pour des opérations inhabituelles.
4. L'autorité de contrôle s'assure que les banques chargent explicitement un cadre supérieur de veiller à ce que leurs politiques et procédures soient au moins conformes aux exigences légales et réglementaires locales en matière de lutte contre le blanchiment d'argent.
5. L'autorité de contrôle s'assure que les banques disposent de procédures claires, communiquées à tout le personnel et permettant à chaque agent de signaler toute opération suspecte au responsable de la conformité en matière de lutte contre le blanchiment d'argent.
6. L'autorité de contrôle s'assure que les banques ont établi des circuits de communication avec la direction et avec une fonction de sécurité interne pour rendre compte des problèmes.
7. En plus d'informer les autorités judiciaires compétentes, les banques signalent à l'autorité de contrôle les activités litigieuses et tout cas important de fraude vis-à-vis de la sécurité, de la solidité ou de la réputation de la banque.
8. La législation, les dispositions réglementaires et/ou les politiques des banques garantissent que la responsabilité d'un membre du personnel ne peut être retenue lorsque celui-ci rapporte en toute bonne foi des activités suspectes au cadre supérieur chargé de ces questions, au responsable de la sécurité interne ou, directement, à l'autorité compétente.
9. L'autorité de contrôle vérifie périodiquement le caractère adéquat des contrôles exercés par les banques en matière de blanchiment d'argent ainsi que de leurs systèmes de prévention, de détection et de notification des fraudes. L'autorité de contrôle est habilitée à tenter une action (poursuite administrative et/ou pénale) contre une banque qui ne respecte pas ses obligations de lutte contre le blanchiment d'argent.
10. L'autorité de contrôle peut communiquer, directement ou indirectement, à ses homologues nationales ou étrangères toute information concernant des activités criminelles suspectées ou avérées.
11. L'autorité de contrôle s'assure que les banques ont défini dans un document leurs critères de déontologie et de professionnalisme et que cette déclaration a été explicitement portée à la connaissance de tout le personnel.

Critères additionnels

1. Les saines pratiques internationales, telles que la conformité aux quarante recommandations formulées en 1990 (révisées en 1996) par le Groupe d'action financière sur le blanchiment d'argent, figurent dans la législation et/ou les dispositions réglementaires.
2. L'autorité de contrôle s'assure que le personnel bancaire est convenablement formé à détecter et à prévenir le blanchiment d'argent.
3. L'autorité de contrôle est légalement tenue d'informer les autorités judiciaires compétentes de toute transaction suspecte.
4. L'autorité de contrôle peut communiquer, directement ou indirectement, au pouvoir judiciaire compétent toute information concernant des activités criminelles suspectées ou avérées.
5. À moins qu'une autre instance n'en soit chargée, l'autorité de contrôle compte parmi ses effectifs des experts en matière d'obligations liées à la lutte contre la fraude financière et le blanchiment d'argent.

Annexe 2: Extraits des recommandations du GAFI

C. Rôle du système financier dans la lutte contre le blanchiment de capitaux

Règles d'identification des clients et de conservation des documents

10. Les institutions financières ne devraient pas tenir de comptes anonymes, ni de comptes sous des noms manifestement fictifs: elles devraient être tenues (par des lois, des règlements, des accords entre autorités de contrôle et institutions financières, ou par des accords d'autodiscipline entre institutions financières) d'identifier, sur la base d'un document officiel ou d'une autre pièce d'identité fiable, leurs clients habituels ou occasionnels, et d'enregistrer cette identité, lorsqu'elles nouent des relations d'affaires ou effectuent des transactions (en particulier lorsqu'elles ouvrent des comptes ou des livrets, lorsqu'elles réalisent des transactions fiduciaires, lorsqu'elles louent des coffres, lorsqu'elles procèdent à des transactions importantes en espèces).

Afin de satisfaire aux exigences d'identification concernant les personnes morales, les institutions financières devraient, si nécessaire, prendre des mesures telles que:

- i) vérifier l'existence et la structure juridiques du client en obtenant de celui-ci ou à partir d'un registre public, ou bien grâce à ces deux sources, une preuve de la constitution en société comprenant des renseignements concernant le nom du client, sa forme juridique, son adresse, les dirigeants et les dispositions régissant le pouvoir d'engager la personne morale;
 - ii) vérifier que toute personne prétendant agir au nom du client est autorisée à le faire et identifier cette personne.
11. Les institutions financières devraient prendre des mesures raisonnables pour obtenir des informations sur l'identité véritable des personnes dans l'intérêt desquelles un compte est ouvert ou une transaction est effectuée, s'il y a le moindre doute sur le fait que ces clients pourraient ne pas agir pour leur propre compte, par exemple dans le cas de sociétés de domicile (c'est-à-dire des institutions, des sociétés, des fondations, des fiducies, etc., qui ne se livrent pas à des opérations commerciales ou industrielles, ou à toute autre forme d'activité commerciale, dans le pays où est situé leur siège social).
12. Les institutions financières devraient conserver pendant au moins cinq ans toutes les pièces nécessaires se rapportant aux transactions effectuées, à la fois nationales et internationales, afin de leur permettre de répondre rapidement aux demandes d'information des autorités compétentes. Ces pièces doivent permettre de reconstituer les transactions individuelles (y compris les montants et les types d'espèces en cause, le cas échéant) de façon à fournir, si nécessaire, des preuves en cas de poursuites pour conduite criminelle.
- Les institutions financières devraient conserver une trace écrite de la justification d'identité de leurs clients (par exemple, copie ou enregistrement des documents officiels comme les passeports, les cartes d'identité, les permis de conduire, ou des documents similaires), les livres de comptes et la correspondance commerciale pendant cinq ans au moins après la clôture du compte.
- Ces documents devraient être à la disposition des autorités nationales compétentes, dans le contexte de leurs poursuites et de leurs enquêtes pénales.
13. Les pays devraient apporter une attention particulière aux menaces de blanchiment de capitaux inhérentes aux technologies nouvelles ou en développement, qui risquent de favoriser l'anonymat, et prendre des mesures supplémentaires, si nécessaire, pour éviter l'utilisation de ces technologies dans les dispositifs de blanchiment de capitaux.

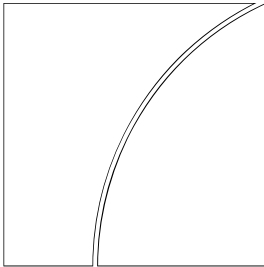
Diligence accrue des institutions financières

14. Les institutions financières devraient apporter une attention particulière à toutes les opérations complexes, inhabituelles, importantes, et à tous les types inhabituels de transactions, lorsqu'elles n'ont pas de cause économique ou licite apparente. L'arrière-plan et l'objet de telles opérations devraient être examinés, dans la mesure du possible; les résultats de cet examen devraient être établis par écrit, et être disponibles pour aider les autorités de contrôle, de détection et de répression, les commissaires aux comptes et les contrôleurs internes ou externes.
15. Si les institutions financières suspectent que des fonds proviennent d'une activité criminelle, elles devraient être obligées de déclarer rapidement leurs soupçons aux autorités compétentes.
16. Les institutions financières, leurs dirigeants et employés devraient être protégés par des dispositions législatives contre toute responsabilité, pénale ou civile, pour violation des règles de confidentialité - qu'elles soient imposées par contrat ou par toute disposition législative, réglementaire ou administrative - si elles déclarent de bonne foi leurs soupçons aux autorités compétentes, même si elles ne savaient pas précisément quelle était l'activité criminelle en question, et même si l'activité illégale soupçonnée n'est pas réellement intervenue.
17. Les institutions financières, leurs dirigeants et employés ne devraient pas avertir leurs clients, ou, le cas échéant, ne devraient pas être autorisés à les avertir, lorsqu'ils portent à la connaissance des autorités compétentes des informations qui sont relatives à ces clients.
18. Les institutions financières déclarant leurs soupçons devraient se conformer aux instructions en provenance des autorités compétentes.
19. Les institutions financières devraient mettre au point des programmes de lutte contre le blanchiment de capitaux, qui devraient comprendre au minimum:
 - i) des politiques, des procédures et des contrôles internes, y compris la désignation de personnes responsables au niveau de la direction générale, et des procédures adéquates lors de l'embauche des employés, de façon à s'assurer qu'elle s'effectue selon des critères exigeants;
 - ii) un programme continu de formation des employés;
 - iii) un dispositif de contrôle interne pour vérifier l'efficacité du système.

Comitato di Basilea
per la vigilanza bancaria

394

Bulletin CFB 44/2003



Dovere di diligenza delle banche nell'identificazione della clientela

Ottobre 2001



BANCA DEI REGOLAMENTI INTERNAZIONALI

Gruppo di lavoro sull'attività bancaria transfrontaliera

Co-Presidenti:

Charles Freeland, Vice Segretario Generale del Comitato di Basilea per la vigilanza bancaria

Colin Powell, Presidente del Gruppo Offshore di autorità di vigilanza bancaria e Presidente della Jersey Financial Services Commission

Bermuda Monetary Authority

Cayman Islands Monetary Authority

Banque de France/Commission Bancaire

Bundesamt für Bankenaufsicht, Germania

Guernsey Financial Services Commission

Banca d'Italia

Financial Services Agency, Giappone

Commission de Surveillance du Secteur Financier,
Lussemburgo

Monetary Authority of Singapore

Commissione federale per le banche, Svizzera

Financial Services Authority, Regno Unito

Board of Governors of the Federal Reserve System

Federal Reserve Bank of New York

Office of the Comptroller of the Currency

Segretariato

D. Munro Sutherland

John Bourbon
Anna McLean

Laurent Ettori

Jochen Sanio
Peter Kruschel

Peter G. Crook (fino all'aprile 2001)
Philip Marr (dall'aprile 2001)

Giuseppe Godano

Kiyotaka Sasaki (fino al luglio 2001)
Hisashi Ono (dal luglio 2001)

Romain Strock

Foo-Yap Siew Hong
Teo Lay Har

Daniel Zuberbühler
Dina Balleyguier

Richard Chalmers

William Ryback

Nancy Bercovici

Jose Tuya
Tanya Smith

Andrew Khoo

Indice

I.	Introduzione	1
II.	Importanza dei requisiti KYC per le autorità di vigilanza e le banche	2
III.	Elementi essenziali dei requisiti KYC	4
1.	Politica di accettazione dei clienti	4
2.	Identificazione del cliente	4
2.1	Requisiti generali	5
2.2	Questioni specifiche	6
2.2.1	Conti intestati a trust, rappresentanti e fiduciari	6
2.2.2	Società veicolo	6
2.2.3	Clienti introdotti da terzi	7
2.2.4	Conti di clienti aperti da intermediari professionisti	7
2.2.5	Persone politicamente esposte	8
2.2.6	Clienti non conosciuti di persona	9
2.2.7	Servizi bancari di corrispondenza	9
3.	Monitoraggio continuativo dei conti e delle operazioni	10
4.	Gestione del rischio	11
IV.	Ruolo delle autorità di vigilanza	12
V.	Applicazione dei requisiti KYC in un contesto transnazionale	12
Allegato 1 – Estratto dal documento <i>Metodologia dei Principi fondamentali per un'efficace vigilanza bancaria</i>		15
Allegato 2 – Estratto dalle Raccomandazioni FATF/GAFI		17

Dovere di diligenza delle banche nell'identificazione della clientela

I. Introduzione

1. Le autorità di vigilanza di tutto il mondo sono sempre più consapevoli dell'importanza di assicurare che le banche di propria pertinenza pongano in atto adeguati controlli e procedure per conoscere i clienti con cui operano. L'esercizio della dovuta diligenza nei confronti della clientela esistente e di nuova acquisizione costituisce un elemento essenziale di tali controlli, in assenza del quale le banche possono esporsi a rischi di reputazione, operativi, legali e di concentrazione, e conseguentemente incorrere in costi finanziari considerevoli.

2. Analizzando i risultati di un'inchiesta interna del 1999 sull'attività bancaria transfrontaliera, il Comitato di Basilea ha rilevato come in numerosi paesi vi siano carenze nelle politiche delle banche per l'identificazione dei clienti ("know-your-customer", KYC). Giudicate in un'ottica di vigilanza, tali politiche mostrano gravi lacune in alcuni paesi, mentre in altri appaiono del tutto assenti. Anche nell'ambito dei paesi con mercati finanziari evoluti gli standard non sono uniformi. Pertanto, il Comitato ha chiesto al Gruppo di lavoro sull'attività bancaria transfrontaliera¹ di esaminare le procedure KYC attualmente in uso e di elaborare raccomandazioni applicabili alle banche di tutti i paesi. Il rapporto che ne è scaturito è stato pubblicato a fini consultivi nel gennaio 2001. Dopo un'attenta valutazione dei commenti ricevuti, il Gruppo di lavoro ha redatto un nuovo documento riveduto che il Comitato distribuisce oggi su scala mondiale, confidando che lo schema in esso proposto venga assunto come riferimento dalle autorità di vigilanza nella definizione di standard nazionali e dalle banche nella formulazione dei propri programmi. È importante riconoscere che in talune giurisdizioni le pratiche di vigilanza soddisfano già, o vanno addirittura oltre, i requisiti stabiliti nel presente documento e potrebbero quindi non richiedere alcuna modifica.

3. Le procedure KYC sono intimamente collegate alla lotta contro il riciclaggio dei fondi di provenienza illecita, che è essenzialmente di pertinenza della Financial Action Task Force (FATF)². Non è intenzione del Comitato duplicare le iniziative della FATF. Il suo interesse si colloca infatti in una più ampia prospettiva prudenziale. L'applicazione di corrette politiche e procedure KYC è essenziale al fine di salvaguardare la sicurezza e la solidità delle banche, nonché l'integrità del sistema bancario. Il Comitato di Basilea e il Gruppo offshore di autorità di vigilanza bancaria (Gruppo offshore) continueranno a sostenere fermamente l'adozione e l'applicazione pratica delle raccomandazioni FATF, specie quelle riguardanti le banche, ed è loro intendimento che gli standard stabiliti in questo documento siano coerenti con tali raccomandazioni. Il Comitato di Basilea e il Gruppo offshore considereranno inoltre l'adozione di eventuali requisiti più stringenti introdotti dalla FATF in sede di revisione delle sue 40 Raccomandazioni. Di conseguenza, il Gruppo di lavoro rimarrà in stretto contatto con la FATF per seguire attentamente le sue deliberazioni.

4. L'approccio del Comitato di Basilea al KYC si pone in un'ottica di vigilanza più ampia, non incentrata unicamente sulla lotta al riciclaggio di proventi illeciti. L'applicazione di corrette procedure KYC va riguardata come elemento cruciale di un'efficace gestione dei rischi bancari. Le salvaguardie in questo ambito non concernono soltanto l'apertura dei conti e la tenuta della documentazione, ma implicano anche la formulazione di una politica per l'accettazione della clientela e di un programma

¹ Gruppo congiunto formato da membri del Comitato di Basilea e del Gruppo offshore di autorità di vigilanza bancaria.

² La FATF (nota anche come "Gruppo di azione finanziaria", GAFI) è un ente intergovernativo, costituito da 29 paesi membri e due organismi regionali, che elabora e promuove, a livello sia nazionale che internazionale, direttive per combattere il riciclaggio di denaro. Essa opera in stretta collaborazione con altri organismi internazionali attivi in questo campo, quali l'Office for Drug Control and Crime Prevention delle Nazioni Unite, il Consiglio d'Europa, l'Asia-Pacific Group on Money Laundering e la Caribbean Financial Action Task Force. La FATF definisce il riciclaggio di denaro come il trattamento dei proventi di attività delittuose allo scopo di dissimularne l'origine illegale.

articolato per la sua identificazione, che preveda una più scrupolosa diligenza nei riguardi dei conti a maggiore rischio, nonché il loro monitoraggio attivo al fine di rilevare eventuali attività sospette.

5. L'interesse del Comitato di Basilea per una corretta prassi KYC origina dalla sua preoccupazione per l'integrità del mercato ed è stato accentuato dalle perdite dirette e indirette subite da talune banche in seguito alla loro mancanza di diligenza nell'applicare adeguate procedure. Probabilmente tali perdite avrebbero potuto essere evitate, e i danni in termini di reputazione notevolmente ridotti, se le istituzioni in questione avessero adottato efficaci programmi KYC.

6. Il presente documento rafforza i principi stabiliti in precedenti pubblicazioni del Comitato, fornendo orientamenti più precisi riguardo agli elementi essenziali delle procedure KYC e alla loro applicazione pratica. Nell'elaborare le linee guida il Gruppo di lavoro si è basato sulle pratiche vigenti nei paesi membri e ha tenuto conto dell'evoluzione in campo prudenziale. Gli elementi essenziali presentati in questo documento vanno intesi come requisiti minimi applicabili a tutte le banche su scala mondiale. Tali requisiti potranno essere integrati e/o rafforzati mediante prescrizioni addizionali commisurate ai rischi presenti in determinate istituzioni e nel sistema bancario di singoli paesi. Ad esempio, un'accresciuta diligenza è richiesta per i conti a più alto rischio o per le banche che mirano specificatamente ad attirare clienti dotati di patrimoni di ingente ammontare. In varie sezioni del documento sono contenute raccomandazioni per l'adozione, ove applicabile, di criteri di diligenza più stringenti nelle aree di maggiore rischio all'interno di una banca.

7. La necessità di rigorosi standard di diligenza riguardo alla clientela non concerne soltanto le banche. Il Comitato di Basilea è del parere che raccomandazioni analoghe vadano formulate anche per le istituzioni finanziarie non bancarie e per gli intermediari professionisti che operano in ambito finanziario, come avvocati e commercialisti.

II. Importanza dei requisiti KYC per le autorità di vigilanza e le banche

8. La FATF e altri gruppi internazionali hanno lavorato intensamente sulla problematica KYC, e le 40 Raccomandazioni emanate dalla FATF per combattere il riciclaggio di denaro³ trovano riconoscimento e attuazione su scala internazionale. Non è intenzione del presente documento duplicare tale lavoro.

9. Al tempo stesso, l'applicazione di rigorose procedure KYC ha particolare rilevanza ai fini della sicurezza e solidità delle banche, in quanto essa:

- contribuisce a proteggere la reputazione delle istituzioni e l'integrità dei sistemi bancari, limitando il pericolo che gli enti creditizi diventino veicoli o vittime di crimini finanziari e subiscano conseguenti danni di immagine;
- è parte essenziale di una sana gestione del rischio (fornendo tra l'altro la base per individuare, limitare e controllare le esposizioni al rischio insite negli elementi attivi e passivi del patrimonio, ivi compresi gli averi ricevuti in amministrazione).

10. L'inadeguatezza o l'assenza di standard KYC può esporre le banche a gravi rischi nei confronti della clientela e delle controparti, e in particolare a **rischi di reputazione, operativi, legali e di concentrazione**. Va rilevato che tutti questi rischi sono correlati. Nondimeno, ognuno di essi può comportare ingenti oneri finanziari (causati ad esempio da ritiro di depositi, revoca di linee creditizie interbancarie, richiesta di danni, costi di investigazione, misure cautelative e sequestrative a carico di cespiti patrimoniali, perdite su crediti), nonché costringere il management a dedicare tempo ed energie alla risoluzione dei problemi che ne conseguono.

11. Il **rischio di reputazione** costituisce una grave minaccia per le banche, poiché la natura stessa della loro attività presuppone il mantenimento della fiducia dei depositanti, dei creditori e del mercato in generale. Il rischio di reputazione può definirsi come la possibilità che la diffusione di notizie negative, siano esse veritiere o meno, concernenti le modalità di gestione o le connessioni di una banca intacchino la fiducia nella sua integrità. Le banche sono particolarmente esposte a questo

³ Si vedano le Raccomandazioni 10-19 della FATF, riportate nell'Allegato 2.

tipo di rischio in quanto possono facilmente diventare strumento o vittima di attività illecite compiute da propri clienti. Esse devono proteggersi esercitando una vigilanza costante mediante l'applicazione di rigorose procedure KYC. Particolari rischi di reputazione possono derivare dalle attività detenute in amministrazione o su base fiduciaria.

12. Il **rischio operativo** è definibile come il rischio di perdite dirette o indirette derivanti da disfunzioni a livello di procedure, personale e sistemi interni, oppure da eventi esogeni. Nel contesto dell'identificazione della clientela il rischio operativo è per lo più collegato a deficienze nell'attuazione dei programmi, all'inefficacia delle procedure di controllo e al mancato esercizio della dovuta diligenza. La percezione da parte del pubblico che una banca non sia capace di gestire in modo efficace il proprio rischio operativo può compromettere o influenzare negativamente l'attività dell'istituzione.

13. Il **rischio legale** è il rischio che azioni legali, sentenze avverse o contratti rivelatisi giuridicamente inefficaci possano pregiudicare o perturbare l'operatività o le condizioni di una banca. Le banche possono essere chiamate in giudizio per l'inosservanza di requisiti cogenti in materia di identificazione dei clienti o per il mancato esercizio della dovuta diligenza e, in conseguenza di ciò, subire multe, procedimenti penali e sanzioni speciali inflitte dalle autorità di vigilanza. Di fatto, per una banca coinvolta in un procedimento giudiziario le implicazioni finanziarie negative possono andare ben oltre i semplici costi legali. Le banche sono nell'impossibilità di tutelarsi efficacemente contro tali rischi legali se non esercitano la dovuta diligenza nell'identificare i propri clienti e nel conoscere le attività che questi svolgono.

14. Sul piano prudenziale i timori circa il **rischio di concentrazione** riguardano essenzialmente il lato degli impieghi bancari. Di regola, le autorità di vigilanza non soltanto richiedono alle banche di disporre di sistemi informativi che consentano loro di individuare le concentrazioni dei fidi, ma solitamente pongono anche limiti all'esposizione verso singoli mutuatari o gruppi di mutuatari collegati. Se una banca non conosce esattamente l'identità dei suoi affidati e le loro connessioni con altri clienti, essa non sarà in grado di misurare il rischio di concentrazione. Ciò assume particolare rilevanza nel contesto dei prestiti a entità consociate e a soggetti collegati.

15. Dal lato del passivo il rischio di concentrazione è intimamente correlato al rischio di finanziamento, e in particolare al rischio di un imprevisto ritiro anticipato di fondi da parte di grandi depositanti, con effetti potenzialmente deleteri per la liquidità della banca. Il rischio di finanziamento tende a essere più elevato nel caso degli istituti di dimensioni modeste o meno attivi sui mercati all'ingrosso. Per poter analizzare le concentrazioni dal lato della provvista è necessaria una buona conoscenza delle caratteristiche dei depositanti, intendendo con ciò non soltanto l'identità, ma anche la misura in cui le loro azioni possono essere interrelate. È essenziale che nelle banche di piccole dimensioni i responsabili della gestione del passivo non si limitino a conoscere i maggiori depositanti, ma mantengano con essi rapporti assidui, onde evitare di perdere la disponibilità dei loro fondi nei momenti critici.

16. Non di rado i clienti hanno più conti nella stessa banca, ma presso sportelli situati in paesi diversi. Al fine di gestire efficacemente i rischi di reputazione, di conformità e legali che possono risultare dall'esistenza di tali conti, le banche dovrebbero essere in grado di aggregarne e monitorarne le giacenze e i movimenti su una base pienamente consolidata a livello mondiale, a prescindere dalla forma tecnica (strumenti in bilancio o fuori bilancio, fondi in amministrazione o depositi fiduciari) in cui sono detenuti gli averi.

17. Il Comitato di Basilea e il Gruppo offshore di autorità di vigilanza bancaria sono fermamente convinti che l'applicazione di rigorose procedure KYC debba essere parte integrante dei sistemi di gestione del rischio e di controllo interno di tutte le banche del mondo. Le autorità di vigilanza nazionali sono tenute ad assicurare che le istituzioni di propria pertinenza attuino requisiti minimi di diligenza e controlli interni idonei a fornire una conoscenza adeguata dei propri clienti. I codici di comportamento volontari⁴ emanati da organismi o associazioni di categoria possono essere di grande utilità come complemento delle direttive regolamentari, fornendo alle banche indicazioni pratiche in ordine a specifiche questioni operative. Essi non possono tuttavia sostituirsi alle prescrizioni ufficiali.

⁴ Un esempio di codice di questo genere è fornito dalle "Global anti-money-laundering guidelines for Private Banking" (note anche come "principi Wolfsberg"), redatte nell'ottobre 2000 da dodici grandi banche con una importante operatività nel settore del private banking.

III. Elementi essenziali dei requisiti KYC

18. Le linee guida del Comitato di Basilea in merito alle politiche KYC sono contenute nei seguenti tre documenti, che riflettono l'evoluzione dell'approccio prudenziale nel corso del tempo. Il documento *Prevenzione dell'utilizzo del sistema bancario per il riciclaggio di fondi di provenienza illecita*, pubblicato nel 1988, enuncia i principi etici basilari e incoraggia le banche a porre in essere efficaci procedure per identificare la clientela, a rifiutare l'esecuzione di transazioni sospette e a collaborare con le autorità giudiziarie e di polizia. I *Principi fondamentali per un'efficace vigilanza bancaria* del 1997 stabiliscono, nel quadro di una più ampia analisi dei controlli interni, che le banche dovrebbero adottare politiche, prassi e procedure adeguate, fra cui rigorose regole per l'identificazione della clientela; in particolare, le autorità di vigilanza dovrebbero incoraggiare l'adozione delle raccomandazioni della FATF. Esse riguardano l'identificazione dei clienti e la conservazione dei relativi documenti, un'accresciuta diligenza da parte delle istituzioni finanziarie nell'individuare e segnalare le operazioni sospette, nonché le misure da applicare nei rapporti con i paesi in cui vigono prescrizioni inadeguate contro il riciclaggio di capitali illeciti. Il documento *Metodologia dei Principi fondamentali per un'efficace vigilanza bancaria* del 1999 elabora ulteriormente tali Principi enunciando una serie di criteri essenziali e integrativi (nell'Allegato 1 sono riportati i passaggi rilevanti tratti dai due documenti).

19. A ogni banca dovrebbe essere richiesto di disporre di "adeguate politiche, prassi e procedure per promuovere un elevato standard etico e professionale e per impedire che la banca si presti, con o senza intenzionalità, a essere utilizzata da soggetti criminali"⁵. Nei programmi KYC delle banche andrebbero incorporati determinati elementi essenziali. Questi inizierebbero dalle procedure di gestione e controllo del rischio e comprenderebbero 1) la politica di accettazione della clientela, 2) l'identificazione del cliente, 3) il regolare monitoraggio dei conti ad alta rischiosità e 4) la gestione del rischio. Le banche non dovrebbero limitarsi ad accertare l'identità dei clienti, ma dovrebbero anche monitorare i movimenti dei conti al fine di individuare le transazioni che appaiono anomale avuto riguardo al tipo di cliente o di conto. I requisiti KYC dovrebbero costituire un elemento centrale delle procedure di gestione e controllo del rischio ed essere integrati da regolari verifiche di conformità e revisioni interne. La portata dei programmi KYC che vanno oltre questi elementi essenziali dovrebbe essere adeguata al grado di rischio.

1. Politica di accettazione dei clienti

20. Le banche dovrebbero definire chiare politiche e procedure per l'accettazione della clientela, tra cui una descrizione dei tipi di clienti che comportano presumibilmente rischi superiori alla media. A tale riguardo andrebbero considerati fattori come il background, il paese d'origine e la posizione pubblica o di elevato profilo del cliente, la titolarità di conti collegati, l'attività economica svolta e altri indicatori di rischio. Le banche dovrebbero adottare politiche e procedure di accettazione differenziate con requisiti di diligenza progressivamente più stringenti in funzione della rischiosità del cliente. Ad esempio, per l'accensione di un conto da parte di una persona con una normale attività lavorativa e un saldo modesto potrebbe essere prescritta l'osservanza dei requisiti più elementari. È infatti importante che i criteri di accettazione della clientela non siano così restrittivi da precludere l'accesso ai servizi bancari da parte del grande pubblico, e in particolare delle persone economicamente o socialmente sfavorite. Per converso, è essenziale che venga esercitata una scrupolosa diligenza nei confronti di un soggetto con ingenti disponibilità di origine incerta. La decisione di allacciare rapporti di affari con clienti a più alto rischio, come le persone "politicamente esposte" (cfr. sezione 2.2.5), dovrebbe essere presa unicamente a livello di alta direzione.

2. Identificazione del cliente

21. L'identificazione del cliente è un elemento essenziale dei requisiti di diligenza. Ai fini del presente documento si intende per cliente:

⁵ *Metodologia dei Principi fondamentali per un'efficace vigilanza bancaria*, Criterio essenziale 1.

- ogni persona fisica o giuridica che intrattiene, o nell'interesse della quale è intrattenuto (titolare effettivo), un conto presso la banca;
- il beneficiario di transazioni effettuate da intermediari professionisti;
- ogni persona fisica o giuridica associata a una transazione finanziaria che possa comportare per la banca un rilevante rischio di reputazione o di altro tipo.

22. Le banche dovrebbero istituire una procedura sistematica di identificazione dei nuovi clienti ed evitare di stabilire relazioni finanziarie con essi finché la loro identità non sia stata verificata in modo soddisfacente.

23. Le banche dovrebbero disporre di politiche "documentate e applicate di fatto per l'identificazione dei clienti e dei soggetti che agiscono per loro conto"⁶. I documenti più idonei a verificare l'identità dei clienti sono quelli più difficili da ottenere illegalmente o da contraffare. Particolare attenzione è richiesta nel caso della clientela non residente, e in nessuna circostanza la banca dovrebbe eludere la procedura di identificazione soltanto perché il nuovo cliente non può presentarsi di persona. La banca dovrebbe sempre chiedersi per quale ragione il cliente ha scelto di aprire un conto in una giurisdizione estera.

24. Il procedimento di identificazione del cliente si applica naturalmente all'inizio della relazione. Ma affinché i dati rimangano aggiornati e pertinenti, è necessario che le banche verifichino regolarmente la documentazione esistente⁷. Un momento opportuno per tale verifica è quello in cui viene effettuata una transazione importante, oppure sono modificati in modo significativo gli standard per la documentazione della clientela, oppure interviene un cambiamento sostanziale nel modo in cui è utilizzato un conto. Tuttavia, ogniqualevolta una banca ritenga di non possedere sufficienti informazioni su un dato cliente, essa dovrebbe compiere i passi necessari affinché tutti i dati pertinenti siano ottenuti il più presto possibile.

25. Le istituzioni che offrono servizi di private banking sono particolarmente esposte al rischio di reputazione e dovrebbero pertanto esercitare una più scrupolosa diligenza in questo tipo di operazioni. I conti di private banking, che per loro natura comportano un alto grado di riservatezza, possono essere accessi a nome di un individuo, di un'impresa, di un trust, di un intermediario o di una società di investimento personalizzato. In ognuno di questi casi la banca può esporsi a un rischio di reputazione se non applica con diligenza le procedure di identificazione stabilite. Tutti i nuovi clienti e i nuovi conti dovrebbero essere approvati da almeno una persona di appropriato livello gerarchico, oltre al responsabile delle relazioni di private banking. Qualora per questa sfera di attività siano previste particolari salvaguardie interne a tutela della riservatezza, la banca dovrà comunque assicurarsi che sui clienti e sulle operazioni in questione possano essere esercitati uno scrutinio e un monitoraggio almeno equivalenti, ad esempio mediante verifiche da parte degli addetti al controllo di conformità e dei revisori.

26. Le banche dovrebbero definire "chiare regole che stabiliscono la documentazione da tenersi sull'identificazione del cliente e sulle singole transazioni, nonché il suo periodo di conservazione"⁸. Questa prassi è essenziale affinché le banche possano seguire la relazione con il cliente, conoscere le sue attività correnti e, se necessario, produrre evidenze in caso di controversie, azioni legali o indagini finanziarie che potrebbero sfociare in procedimenti penali. Quale ovvia e naturale prosecuzione della procedura di identificazione, la banca dovrebbe richiedere al cliente i documenti necessari per la sua identificazione e conservarne copia per almeno cinque anni dopo la chiusura del conto. Anche le evidenze di tutte le transazioni finanziarie andrebbero tenute per almeno cinque anni dal giorno in cui hanno avuto luogo.

2.1 Requisiti generali

27. Le banche devono poter ottenere tutte le informazioni ritenute necessarie per stabilire in modo pienamente soddisfacente l'identità di ciascun nuovo cliente, così come la finalità e la prevista

⁶ *Metodologia dei Principi fondamentali per un'efficace vigilanza bancaria*, Criterio essenziale 2.

⁷ L'applicazione di nuovi standard KYC ai conti già esistenti è attualmente all'esame della FATF.

⁸ *Metodologia dei Principi fondamentali per un'efficace vigilanza bancaria*, Criterio essenziale 2.

tipologia della relazione finanziaria. La portata e la natura delle informazioni dipenderanno dalle caratteristiche del richiedente (privato, impresa, ecc.) e dalla presunta entità del saldo. Le autorità di vigilanza nazionali sono invitate a fornire criteri guida che assistano le banche nella definizione delle procedure di identificazione. Il Gruppo di lavoro ha intenzione di definire gli elementi essenziali dei requisiti di identificazione della clientela.

28. Allorché un conto è già stato aperto, ma nella relazione bancaria sopravvivono problemi di verifica irrisolvibili, la banca dovrebbe chiudere il conto stesso e restituire i fondi alla fonte da cui le sono pervenuti⁹.

29. Sebbene la provenienza delle disponibilità iniziali da un conto intestato al nuovo cliente presso un'altra banca che applica gli stessi standard KYC possa fornire una certa assicurazione, va comunque considerata la possibilità che tale banca abbia preteso l'estinzione del conto a causa di dubbi sulla liceità delle attività svolte dal titolare. Ovviamente, i clienti hanno il diritto di spostare fondi da un istituto all'altro. Tuttavia, se una banca ha motivo di credere che a un richiedente sia stato negato l'accesso ai servizi di un altro istituto, essa dovrebbe applicare nei suoi confronti procedure di diligenza più stringenti.

30. Le banche non dovrebbero mai accettare di aprire un conto o di effettuare operazioni con un soggetto che persista nel mantenere l'anonimato o fornisca un nominativo fittizio. I conti cifrati confidenziali¹⁰ non dovrebbero funzionare come conti anonimi, bensì essere soggetti esattamente alle stesse procedure KYC che si applicano a tutti gli altri conti, quand'anche i controlli siano compiuti da personale selezionato. I conti cifrati possono sì offrire una protezione addizionale per l'identità del titolare, ma questa deve essere nota a un sufficiente numero di funzionari della banca affinché sia esercitata la dovuta diligenza. Tali conti non dovrebbero quindi in nessun caso essere utilizzati per celare l'identità del cliente ai responsabili del controllo interno di conformità o alle autorità di vigilanza.

2.2 Questioni specifiche

31. Restano da affrontare talune questioni più di dettaglio inerenti all'identificazione del cliente. Parte di esse è attualmente all'esame della FATF nel quadro di una revisione generale delle sue 40 Raccomandazioni, e il Gruppo di lavoro riconosce la necessità di un approccio coerente con i principi della FAFT.

2.2.1 Conti intestati a trust, rappresentanti e fiduciari

32. I conti intestati a trust, rappresentanti e fiduciari possono essere utilizzati per eludere le procedure di identificazione. Sebbene in determinate circostanze sia lecito prevedere un margine di sicurezza addizionale per tutelare la riservatezza dei legittimi clienti di private banking, è essenziale che sia ben compresa la vera natura della relazione. Le banche dovrebbero accertare se il cliente assume il nome di un altro soggetto, se agisce da prestanome, oppure se opera per conto di una terza persona in qualità di amministratore fiduciario, rappresentante o in altra veste. In questi casi è indispensabile che la banca ottenga sufficienti evidenze sull'identità dell'intermediario e del soggetto per conto del quale questi agisce, nonché informazioni dettagliate sulla natura del rapporto fiduciario o di rappresentanza. In particolare, il procedimento di identificazione di un trust dovrebbe comprendere gli affidatari (trustees), i disponenti/affidanti (settlers/grantors) e i beneficiari (beneficiaries)¹¹.

2.2.2 Società veicolo

33. Le banche devono vigilare affinché le imprese societarie non siano utilizzate da persone fisiche come strumento per manovrare conti anonimi. Taluni veicoli di gestione personalizzata di

⁹ Fatta salva la legislazione nazionale in materia di transazioni sospette.

¹⁰ In un conto cifrato, il nome del titolare è noto alla banca, ma viene sostituito da un codice alfanumerico nella successiva documentazione.

¹¹ I beneficiari dovrebbero essere per quanto possibile identificati allorché sono individuabili. Si riconosce che non sempre è possibile individuare fin dall'inizio i beneficiari di un trust. Ad esempio, i beneficiari possono essere persone non ancora nate, oppure diventare tali solo al verificarsi di un determinato evento. Inoltre, ai beneficiari rientranti in specifiche categorie (come nel caso di un fondo pensione aziendale) possono essere opportunamente applicati i criteri enunciat per i conti collettivi, di cui ai paragrafi 38-39.

patrimoni, come le società d'affari internazionali, possono rendere difficile la corretta identificazione dei clienti e dei titolari effettivi. Una banca dovrebbe conoscere bene la struttura della società, determinare l'origine dei fondi e individuare i proprietari effettivi o i soggetti che hanno il controllo sui fondi.

34. Particolare cautela deve essere esercitata nell'instaurare relazioni finanziarie con società aventi azionisti prestanome o azioni al portatore. Per le società di questo tipo è essenziale che siano acquisite soddisfacenti evidenze sull'identità dei proprietari effettivi. Nel caso di società con capitale costituito in larga parte da azioni al portatore è richiesta un'accresciuta vigilanza. Una banca può infatti essere del tutto ignara degli eventuali trasferimenti di tali azioni. Spetta alle banche porre in atto efficaci procedure per monitorare l'identità dei proprietari effettivi di portafogli rilevanti. Ciò potrebbe implicare che la banca immobilizzi le azioni, ad esempio trattenendole in custodia.

2.2.3 Clienti introdotti da terzi

35. Le procedure di identificazione possono comportare un dispendio di tempo, ed è naturale che le banche desiderino limitare gli inconvenienti causati alla nuova clientela. Di conseguenza, in alcuni paesi è invalsa l'abitudine di fare assegnamento sulle procedure applicate da altri istituti o da agenti che fungono da referenza per i clienti proposti. Questa prassi comporta tuttavia il rischio che le banche confidino in misura eccessiva nelle procedure di diligenza che esse presumono siano state applicate dai terzi proponenti. Il fatto di contare sull'espletamento degli obblighi di diligenza da parte dell'agente che funge da referenza, per quanto autorevole egli sia, non esime in alcun modo le banche dalla responsabilità di conoscere i propri clienti e le loro attività. In particolare, le banche non dovrebbero fare affidamento su agenti che applicano standard KYC meno rigorosi di quelli su cui sono basate le proprie procedure di identificazione o che non sono disposti a fornire copia della documentazione attestante l'esercizio della dovuta diligenza.

36. Il Comitato di Basilea raccomanda alle banche che si avvalgono di agenti per la presentazione di un cliente di vagliare accuratamente la loro "onorabilità e professionalità" e di assicurarsi che essi esercitino la dovuta diligenza secondo i criteri stabiliti in questo documento. È comunque alla banca che compete la responsabilità ultima di conoscere i propri clienti. Le banche dovrebbero basarsi sui seguenti criteri per stabilire l'idoneità di un agente¹²:

- esso deve conformarsi ai requisiti minimi di diligenza per l'identificazione della clientela stabiliti nel presente documento;
- le procedure di diligenza dell'agente devono essere altrettanto rigorose quanto quelle che avrebbe applicato al cliente la banca stessa;
- la banca deve essere certa dell'affidabilità dei sistemi impiegati dall'agente per verificare l'identità del cliente;
- la banca deve concordare con l'agente di poter verificare in ogni momento se esso ha esercitato la dovuta diligenza;
- tutti i dati identificativi rilevanti e i documenti concernenti l'identità del cliente devono essere immediatamente sottoposti dall'agente alla banca, la quale è tenuta a esaminare accuratamente la documentazione ricevuta. Tali informazioni devono essere accessibili all'autorità di vigilanza e all'organo di investigazione finanziaria, o autorità di polizia equivalente, cui sia stato conferito il necessario potere legale.

Inoltre, la banca che fa ricorso a un agente dovrebbe effettuare periodiche verifiche per assicurarsi che questi continui a conformarsi ai criteri sopra enunciati.

2.2.4 Conti di clienti aperti da intermediari professionisti

37. Allorché una banca sa per certo o ha motivo di ritenere che il conto aperto da un intermediario professionista è gestito in favore di un dato cliente, essa deve pretendere di conoscere l'identità di quest'ultimo.

¹² La FATF sta attualmente esaminando i criteri di idoneità da applicare agli agenti che presentano un cliente.

38. Le banche detengono spesso conti "collettivi" gestiti da intermediari professionisti in favore di enti, come fondi comuni di investimento, fondi pensione e fondi cassa. Esse intrattengono anche conti collettivi intestati ad avvocati o agenti di cambio in cui sono versati fondi detenuti in deposito o custodia per vari tipi di clienti. Qualora tali fondi non siano indivisi, bensì ripartiti in "sottoconti" attribuibili a singoli beneficiari, questi ultimi devono essere identificati individualmente.

39. Nel caso in cui i fondi siano indivisi, la banca dovrebbe identificare i beneficiari. Possono esservi circostanze in cui la banca non abbia bisogno di risalire a monte dell'intermediario, come ad esempio quando quest'ultimo è tenuto a osservare le stesse norme e procedure prudenziali e anticiclaggio e, in particolare, soggiace agli stessi requisiti di diligenza per l'identificazione della clientela. Le autorità di vigilanza nazionali dovrebbero chiaramente definire le circostanze particolari di cui sopra. Le banche dovrebbero accettare tali conti soltanto se sono in grado di appurare che l'intermediario esercita la dovuta diligenza e dispone di sistemi e controlli per allocare gli averi depositati nel conto collettivo ai rispettivi beneficiari. Nel valutare le procedure di diligenza poste in atto dall'intermediario la banca dovrebbe applicare i criteri enunciati nel paragrafo 36 in relazione agli agenti che presentano un cliente, al fine di determinare se l'intermediario stesso offre sufficienti garanzie di affidabilità.

40. Se l'intermediario non è abilitato a fornire alla banca le necessarie informazioni sui beneficiari, come nel caso degli avvocati¹³ vincolati dal segreto professionale, oppure non soggiace a requisiti di diligenza equivalenti a quelli stabiliti nel presente documento o alle disposizioni previste dalle norme anticiclaggio, la banca non dovrebbero consentirgli di aprire un conto.

2.2.5 Persone politicamente esposte

41. Le relazioni d'affari con individui che ricoprono importanti cariche pubbliche e con persone o imprese ad essi chiaramente collegate possono esporre le banche a notevoli rischi di reputazione e/o legali. Con persone "politicamente esposte" (PPE) si intendono gli individui che sono o erano preposti ad alte funzioni pubbliche, come Capi di Stato o di Governo, personalità politiche, quadri superiori della Pubblica amministrazione, della magistratura e delle forze armate, dirigenti di imprese pubbliche e importanti esponenti di partiti politici. Vi è sempre la possibilità, specie nei paesi in cui la corruzione è fenomeno diffuso, che tali persone abusino dei propri poteri per trarre illeciti guadagni da atti di concussione, malversazione, ecc.

42. L'accettazione e gestione di fondi di PPE corrotte reca grave danno alla reputazione della banca e rischia di pregiudicare la fiducia del pubblico negli standard etici di un intero centro finanziario, poiché solitamente i casi del genere sono seguiti con grande attenzione dai media e suscitano forti reazioni politiche, anche se l'origine illecita degli averi è spesso difficilmente comprovabile. Inoltre, le banche possono essere soggette a costose richieste di informazioni e a provvedimenti sequestrativi a opera delle autorità di polizia o giudiziarie (anche nel quadro di procedure di mutua assistenza giuridica internazionale in materia penale), nonché subire azioni per il risarcimento di danni intentate dallo Stato in questione o dalle vittime di un regime. In determinate circostanze, anche la banca stessa e/o i suoi funzionari possono incorrere nell'accusa di riciclaggio di proventi illeciti, ove risulti che sapevano o avrebbero dovuto sapere che i fondi originavano da corruzione o da altri atti delittuosi.

43. Alcuni paesi hanno recentemente modificato, o stanno modificando, la propria normativa al fine di perseguire penalmente la corruzione attiva di funzionari pubblici esteri in linea con la relativa convenzione internazionale¹⁴. In tal modo, gli atti di corruzione all'estero vengono a configurare una presunzione di reato in materia di riciclaggio di fondi illeciti, attivando l'applicazione di tutte le prescrizioni anticiclaggio (come la segnalazione di transazioni sospette, il divieto di informare il cliente, il congelamento interno di fondi, ecc.). Ma anche in difetto di una tale base esplicita di diritto penale, è chiaramente indesiderabile, eticamente scorretto e incompatibile con i requisiti di onorabilità e di professionalità che una banca accetti o mantenga una relazione finanziaria qualora essa sappia o debba presumere che i fondi traggono origine da corruzione, concussione o peculato. Per una banca

¹³ La FATF sta rivedendo le procedure KYC da applicarsi ai conti aperti da avvocati su incarico dei clienti.

¹⁴ Si veda la Convenzione OCSE su *Combating Bribery of Foreign Public Officials in International Business Transactions*, adottata dalla Negotiating Conference il 21 novembre 1997.

che stia considerando una relazione d'affari con un individuo che essa supponga essere una PPE è una necessità imprescindibile identificare pienamente tale individuo, nonché le persone e le imprese ad esso chiaramente collegate.

44. Le banche dovrebbero ottenere sufficienti informazioni dall'interessato e verificare le informazioni disponibili pubblicamente per stabilire se il nuovo cliente sia o meno una PPE. In caso affermativo le banche dovrebbero accertare l'origine dei fondi prima di acconsentire all'accensione di un conto. La decisione in merito dovrebbe essere presa a livello di alta direzione.

2.2.6 *Clienti non conosciuti di persona*

45. Alle banche è sempre più spesso richiesto di aprire conti a favore di clienti che non si presentano di persona. Il fenomeno, che in passato riguardava tipicamente la clientela non residente, negli ultimi tempi ha assunto assai maggiore importanza con la diffusione dei servizi bancari postali, telefonici ed elettronici. Le banche dovrebbero sottoporre tale clientela "remota" agli stessi requisiti di identificazione e di monitoraggio continuativo applicati ai clienti con i quali ha un contatto diretto. Una questione sorta in tale contesto riguarda la possibilità di una verifica indipendente a opera di una parte terza di chiara fama. L'intera problematica inerente all'identificazione della clientela remota viene attualmente discussa in seno alla FATF, oltre a essere oggetto di esame nel quadro dell'emendamento della Direttiva CEE del 1991.

46. Un tipico esempio di cliente remoto è la persona che intenda effettuare operazioni bancarie elettroniche tramite Internet o tecnologie analoghe. I servizi bancari elettronici comprendono ormai una vasta gamma di prodotti offerti in rete. La natura impersonale e transnazionale di tali servizi, congiunta alla loro rapidità di esecuzione, crea inevitabilmente problemi per l'identificazione e la verifica del cliente. Come principio fondamentale, le autorità di vigilanza si attendono che le banche valutino attivamente i vari rischi posti dalle tecnologie emergenti e applichino procedure di identificazione che tengono adeguatamente conto di tali rischi¹⁵.

47. Sebbene la medesima documentazione possa essere prodotta dalla clientela conosciuta di persona e dalla clientela remota, nel caso di quest'ultima il riscontro dell'identità risulta ovviamente più difficile. Nelle operazioni bancarie telefoniche ed elettroniche il problema della verifica è reso ancora più acuto.

48. Allorché vengono accettati clienti remoti le banche devono:

- applicare procedure di identificazione altrettanto rigorose quanto quelle impiegate per la clientela disponibile a un contatto diretto;
- porre in atto adeguate misure specifiche per attenuare il maggiore rischio.

Sono esempi di misure dirette ad attenuare il rischio:

- certificazione dei documenti presentati;
- richiesta di documenti addizionali rispetto a quelli prescritti alla clientela conosciuta di persona;
- presa di contatto con il cliente su iniziativa autonoma della banca;
- referenze di terzi, ad esempio da parte di un agente soggetto ai requisiti stabiliti al paragrafo 36;
- richiesta che il primo versamento sia effettuato tramite un conto intestato al cliente presso un'altra banca che applica gli stessi requisiti di diligenza.

2.2.7 *Servizi bancari di corrispondenza*

49. Per servizi bancari di corrispondenza si intende la prestazione di servizi da parte di una banca ("banca mandataria") per conto di un'altra banca ("banca mandante"). I conti di corrispondenza, ampiamente utilizzati su scala mondiale, consentono alle banche di offrire prodotti e servizi che esse

¹⁵ L'Electronic Banking Group del Comitato di Basilea ha pubblicato nel maggio 2001 un rapporto sui principi di gestione del rischio nei servizi bancari elettronici.

non sono in grado di fornire direttamente. Fra i conti di corrispondenza richiedono particolare attenzione quelli che prevedono l'offerta di servizi in giurisdizioni in cui la banca mandante non ha alcuna presenza fisica. In ogni caso, le banche che omettono di applicare a tali conti i dovuti criteri di diligenza si espongono ai vari tipi di rischio sopra descritti e possono venirsi a trovare nella situazione di detenere e/o trasferire fondi collegati a corruzione, frode o altri illeciti.

50. Le banche dovrebbero acquisire sufficienti informazioni sulle proprie mandanti al fine di conoscere pienamente la natura delle loro operazioni. Fra gli aspetti da considerare figurano: informazioni concernenti la direzione della banca mandante, le principali attività da essa svolte e la loro localizzazione, nonché le misure messe in atto per prevenire e individuare il riciclaggio di fondi illeciti; le finalità del conto; l'identità di eventuali terzi che utilizzano i servizi bancari di corrispondenza; la qualità della regolamentazione e della vigilanza bancaria nel paese di insediamento. Le banche dovrebbero stabilire rapporti di corrispondenza con istituzioni estere soltanto se queste sono efficacemente vigilate dalle rispettive autorità. Per parte loro, le banche mandanti dovrebbero applicare rigorose politiche e procedure per l'identificazione e l'accettazione della clientela.

51. In particolare, le banche dovrebbero rifiutare di iniziare o continuare un rapporto di corrispondenza con un'istituzione che abbia sede legale in una giurisdizione nella quale non è materialmente presente e che non sia affiliata a un gruppo finanziario regolamentato ("società di comodo"). Le banche dovrebbero essere particolarmente vigili allorché intrattengono rapporti di corrispondenza con istituti situati in giurisdizioni che non applicano rigorosi requisiti KYC o che sono state designate come "non cooperative" nella lotta contro il riciclaggio di capitali illeciti. Le banche dovrebbero assicurarsi che le proprie corrispondenti applichino i requisiti di diligenza stabiliti nel presente documento in ordine alle operazioni effettuate tramite i conti di corrispondenza.

52. Le banche dovrebbero considerare con particolare attenzione il rischio che i conti di corrispondenza siano utilizzati direttamente da terzi per effettuare operazioni per proprio conto (ad esempio, tramite conti di transito). Per tali meccanismi valgono sostanzialmente le considerazioni applicabili alle operazioni di clienti introdotti su presentazione, e quindi i criteri stabiliti al paragrafo 36.

3. Monitoraggio continuativo dei conti e delle operazioni

53. Il monitoraggio continuativo è una componente essenziale di un rigoroso sistema di procedure KYC. Le banche possono controllare e ridurre efficacemente il rischio soltanto se conoscono la normale e ragionevole movimentazione dei conti dei propri clienti, così da poter individuare le operazioni che si discostano dal profilo consueto. Senza una tale conoscenza esse possono facilmente mancare al dovere di segnalare le operazioni sospette alle autorità appropriate nei casi in cui sono tenute a farlo. La portata del monitoraggio deve essere commisurata al rischio. Per tutti i conti le banche dovrebbero avere in funzione sistemi idonei a individuare attività insolite o sospette. A questo fine possono essere stabiliti limiti di importo per le operazioni in ciascuna classe o categoria di conti, il cui superamento dovrebbe essere considerato con particolare attenzione. Anche certi tipi di operazioni dovrebbero mettere in allerta la banca per la possibilità che il cliente stia svolgendo attività insolite o sospette. Tali sono, ad esempio, le operazioni che non appaiono plausibili dal punto di vista economico o commerciale, oppure che comportano depositi in contante di grande ammontare non giustificati dalla normale e prevedibile attività del cliente. Un'eccessiva movimentazione, non commisurata all'entità del saldo, potrebbe indicare che i fondi sono stati "riciclati" attraverso il conto. Una casistica esemplificativa delle attività sospette può essere di notevole aiuto alle banche e dovrebbe far parte delle procedure e/o direttive adottate da una giurisdizione per la lotta al riciclaggio di proventi illeciti.

54. Il monitoraggio dovrebbe essere rafforzato per i conti a più alto rischio. Ogni banca dovrebbe stabilire indicatori chiave per questi conti, avendo riguardo a vari aspetti, come il paese d'origine del cliente, la provenienza dei fondi, il tipo di operazioni effettuate e altri fattori di rischio. Per i conti in questione:

- le banche dovrebbero assicurarsi di disporre di adeguati sistemi informativi per la direzione, affinché ai dirigenti e ai responsabili del controllo di conformità siano forniti con tempestività i dati necessari per identificare, analizzare e sorvegliare efficacemente i movimenti del conto. Fra le segnalazioni potenzialmente necessarie figurano eventuali lacune nella documentazione prescritta per l'apertura del conto, operazioni a valere sul conto di un cliente che appaiono anomale e presentazione complessiva di tutti i rapporti del cliente con la banca;

- i quadri superiori preposti ai servizi di private banking dovrebbero conoscere bene il profilo soggettivo dei clienti ad alto rischio e seguire con attenzione le fonti di informazioni esterne che li concernono. Le operazioni importanti disposte da questi clienti dovrebbero essere approvate da un alto dirigente;
- le banche dovrebbero definire una chiara politica, fissare direttive, procedure e controlli interni ed esercitare una vigilanza particolare riguardo alle relazioni d'affari con le PPE e i soggetti di elevato profilo, nonché con le persone e le imprese a essi chiaramente collegate o associate¹⁶. Data la possibilità che non tutte le PPE siano individuate come tali fin dall'inizio, o che clienti esistenti acquisiscano soltanto in seguito questo status, dovrebbero essere compiute verifiche regolari almeno della clientela più importante.

4. Gestione del rischio

55. Un efficace programma KYC comprende procedure per un'adeguata supervisione direzionale, sistemi e controlli appropriati, separatezza delle funzioni, formazione professionale e altri aspetti collegati. Il consiglio di amministrazione della banca dovrebbe assumere il fermo impegno di attuare un rigoroso programma KYC, stabilendo le procedure appropriate e accertandosi della loro efficacia. All'interno della banca dovrebbero essere assegnate esplicite responsabilità per assicurare che le direttive e le procedure fissate vengano seguite correttamente e siano quantomeno conformi alle prescrizioni di vigilanza locali. I canali per la segnalazione delle operazioni sospette dovrebbero essere chiaramente specificati in forma scritta e resi noti a tutto il personale. Dovrebbero inoltre essere previste procedure interne per determinare se gli obblighi contemplati dalla normativa sulla segnalazione delle attività sospette impongano alla banca di notificare una data operazione alle competenti autorità di polizia, giudiziarie e/o di vigilanza.

56. Alle funzioni di audit interno e di controllo di conformità competono importanti responsabilità nel valutare e assicurare l'osservanza delle direttive e procedure KYC di una banca. Come regola generale, la funzione di controllo di conformità dovrebbe effettuare una valutazione indipendente di tali direttive e procedure, tenuto conto della normativa legale e di vigilanza. Fra i suoi compiti dovrebbe rientrare il monitoraggio continuativo dell'operato del personale mediante verifiche a campione e l'esame delle deroghe, allo scopo di allertare l'alta direzione e il consiglio di amministrazione qualora ritenga che i quadri responsabili non applichino le procedure KYC in modo rigoroso.

57. L'audit interno ha un ruolo importante nel valutare in modo autonomo i sistemi di gestione e controllo del rischio, riferendo al collegio dei sindaci o ad analogo organo di supervisione, mediante relazioni periodiche sull'osservanza delle politiche e procedure KYC, comprese quelle concernenti la formazione del personale. La direzione dovrebbe assicurarsi che la funzione di audit sia adeguatamente dotata di personale competente nella materia in questione. Inoltre, il personale preposto a tale funzione dovrebbe interessarsi attivamente al modo in cui viene dato seguito alle sue osservazioni e critiche.

58. Tutte le banche devono attuare un regolare programma di formazione del personale affinché questo sia adeguatamente addestrato nelle procedure KYC. Tempi e contenuti della formazione per le diverse categorie di personale saranno necessariamente adattati alle esigenze particolari della singola banca. L'impostazione dei corsi differirà a seconda che si tratti di nuovi assunti, operatori di sportello, addetti al controllo di conformità e personale che tratta con i nuovi clienti. Il personale di nuova assunzione deve essere sensibilizzato sull'importanza delle procedure KYC e sui principi fondamentali cui si ispira la banca. I dipendenti di front-office a diretto contatto con il pubblico dovrebbero essere istruiti a verificare l'identità dei nuovi clienti, a espletare su base regolare gli obblighi di diligenza nella gestione dei conti della clientela esistente e a discernere forme di attività sospette. Dovrebbero inoltre essere organizzati regolari corsi di aggiornamento, affinché il personale abbia sempre ben presenti le

¹⁶ Non è realistico attendersi che la banca sia informata o indaghi su ogni lontana relazione familiare, politica o finanziaria di un cliente estero. Le esigenze investigative dipenderanno dalla dimensione o dal movimento dei beni, dalla tipologia delle operazioni, dal background economico, dalla reputazione del paese, dalla plausibilità delle spiegazioni fornite dal cliente, ecc. Va tuttavia notato che le PPE (o meglio, i loro familiari e amici) non si presenteranno necessariamente in tale veste, ma piuttosto come normali professionisti (seppure agiati), dissimulando il fatto che devono la loro posizione elevata in un'impresa legittima unicamente alla relazione privilegiata che intrattengono con il titolare della carica pubblica.

proprie responsabilità e sia informato sui nuovi sviluppi. È essenziale che tutto l'organico interessato comprenda appieno la necessità delle politiche KYC e le applichi in modo rigoroso. Una cultura aziendale che promuova questa comprensione è determinante ai fini di un'efficace attuazione di tali politiche.

59. In molti paesi anche i revisori esterni svolgono un ruolo importante nel monitorare le procedure e i controlli interni delle banche e nell'attestare che essi sono conformi alle prescrizioni di vigilanza.

IV. Ruolo delle autorità di vigilanza

60. Basandosi sugli standard internazionali esistenti, le autorità di vigilanza nazionali dovrebbero emanare direttive intese a disciplinare i programmi KYC delle banche. Gli elementi essenziali enunciati in questo documento dovrebbero fornire alle autorità un chiaro orientamento su come definire o perfezionare la normativa prudenziale nazionale in materia.

61. Oltre a stabilire i requisiti basilari cui devono conformarsi le banche, le autorità di vigilanza sono chiamate ad accertare che queste applichino corrette procedure KYC e operino costantemente nel rispetto degli standard etici e professionali. Le autorità di vigilanza dovrebbero assicurarsi che le banche dispongano di adeguati controlli interni e ottemperino alle prescrizioni prudenziali e regolamentari. Il processo di vigilanza dovrebbe contemplare non soltanto lo scrutinio delle politiche e procedure, ma anche un esame dei dossier clienti e una verifica campionaria dei conti. Le autorità di vigilanza dovrebbero sempre avere la facoltà di accedere a tutta la documentazione relativa ai conti detenuti nella propria giurisdizione, comprese le eventuali analisi effettuate dalla banca per individuare operazioni anomale o sospette.

62. Le autorità di vigilanza hanno il dovere di assicurarsi che le banche di propria pertinenza applichino elevati standard KYC non soltanto al fine di proteggere la sicurezza e la solidità delle singole aziende, ma anche per preservare l'integrità dell'intero sistema bancario nazionale¹⁷. Le autorità dovrebbero far chiaramente intendere che adotteranno le misure appropriate – le quali potranno essere severe e rese note al pubblico, se opportuno – contro le banche e i loro dipendenti che in modo comprovabile violano le direttive interne o le prescrizioni regolamentari. Inoltre, esse dovrebbero assicurarsi che le banche individuino e trattino con particolare cautela le operazioni inerenti a giurisdizioni in cui vigono standard ritenuti inadeguati. La FATF e alcune autorità nazionali hanno predisposto una specifica dei paesi e delle giurisdizioni i cui ordinamenti legali e amministrativi sono considerati non conformi agli standard internazionali per la lotta al riciclaggio di fondi illeciti. Tali indicazioni dovrebbero essere integrate nelle politiche e procedure KYC di una banca.

V. Applicazione dei requisiti KYC in un contesto transnazionale

63. Le autorità di vigilanza di tutto il mondo dovrebbero porre il massimo impegno nel definire e attuare nella propria giurisdizione standard KYC che siano pienamente in linea con i requisiti internazionali, al fine di evitare potenziali "arbitraggi" regolamentari e salvaguardare l'integrità del sistema bancario a livello interno e internazionale. L'attuazione e lo scrutinio di tali standard sono un banco di prova della disponibilità degli organi di vigilanza a cooperare fra di loro in modo concreto e della capacità delle banche di controllare i rischi a livello di gruppo. Si tratta di un compito impegnativo, cui sono chiamate tanto le istituzioni creditizie quanto le autorità di vigilanza.

64. Le autorità di vigilanza si attendono che i gruppi bancari applichino uno standard minimo riconosciuto per le politiche e le procedure KYC sia alle operazioni sull'interno che a quelle transfrontaliere. La supervisione dell'attività bancaria internazionale può essere esercitata in modo efficace soltanto su base consolidata, e i rischi di reputazione e di altro genere non sono confinati al

¹⁷ In molti paesi le autorità di vigilanza sono parimenti tenute a segnalare eventuali operazioni sospette, anomale o illegali che esse rilevino, ad esempio, nel corso di ispezioni in loco.

territorio nazionale. Affinché i programmi KYC operino efficacemente a livello globale, le case madri devono comunicare le proprie politiche e procedure alle filiali e filiazioni estere, ivi comprese entità non bancarie come le società fiduciarie, e predisporre controlli di routine per verificare l'ottemperanza agli standard del paese d'origine e del paese ospitante. Tali controlli di conformità saranno anche sottoposti allo scrutinio dei revisori esterni e delle autorità di vigilanza, ed è quindi importante che la connessa documentazione sia opportunamente conservata e disponibile per i relativi accertamenti. Ai fini della verifica di conformità, gli organi di vigilanza e i revisori esterni dovrebbero in linea generale esaminare i sistemi e i controlli in funzione, nonché i conti della clientela e il monitoraggio delle operazioni nel quadro di accertamenti campionari.

65. Indipendentemente dalle dimensioni della dipendenza estera, dovrebbe essere designato un quadro superiore direttamente responsabile di assicurare che tutto il personale interessato conosca e applichi procedure KYC conformi ai requisiti sia del paese ospitante che del paese d'origine. Sebbene spetti a tale funzionario la responsabilità primaria di questo compito, egli dovrebbe essere coadiuvato dai revisori interni e dagli addetti alla conformità in forza presso la dipendenza stessa ovvero la sede centrale.

66. Qualora i requisiti minimi KYC del paese d'origine e del paese ospitante non siano uniformi, le filiali e filiazioni situate in quest'ultima giurisdizione dovrebbero applicare gli standard più elevati. In generale, non dovrebbero esservi impedimenti a che una banca adotti standard superiori ai requisiti minimi prescritti in loco. Se tuttavia le leggi e i regolamenti del paese ospitante (specie le norme di segretezza) interdicano l'applicazione degli standard KYC del paese d'origine allorché questi sono più restrittivi, le autorità di vigilanza del paese ospitante dovrebbero adoperarsi affinché la normativa nazionale venga modificata. Nel frattempo, le filiali e filiazioni estere dovrebbero conformarsi ai requisiti locali, assicurandosi però che la sede centrale o casa madre e le autorità di vigilanza del paese di quest'ultima siano pienamente informate sulla natura delle difformità.

67. Gli elementi criminali sono facilmente attirati verso le giurisdizioni in cui vigono impedimenti del genere. Pertanto, le banche dovrebbero essere consapevoli del forte rischio di reputazione cui si espongono svolgendo attività in tali giurisdizioni. Le case madri dovrebbero disporre di procedure per analizzare la vulnerabilità delle singole unità operative e predisporre, ove appropriato, salvaguardie addizionali. In casi estremi, le autorità di vigilanza dovrebbero considerare l'opportunità di esercitare controlli aggiuntivi sulle banche attive nelle giurisdizioni in questione e, se del caso, incoraggiare il loro ritiro dalle stesse.

68. Durante le ispezioni in loco le autorità di vigilanza e i revisori del paese d'origine non dovrebbero incontrare nessun ostacolo nell'accertare la conformità della dipendenza con le politiche e procedure KYC. Ciò implicherà l'esame dei registri dei clienti e verifiche a campione di singoli conti. Gli organi di controllo dovrebbero avere accesso alle informazioni sui singoli conti in misura sufficiente a consentire un'adeguata valutazione degli standard KYC applicati e delle procedure di gestione del rischio, senza che vi ostino le norme locali sul segreto bancario. Qualora le autorità del paese d'origine prescrivano la segnalazione consolidata delle concentrazioni dei depositi e dei fidi o la notifica dei fondi in amministrazione, non dovrebbero esservi impedimenti a comunicare tali dati. Inoltre, per poter sorvegliare le concentrazioni dei depositi o i rischi di provvista in relazione ai prelievi, le autorità del paese d'origine potrebbero applicare test di rilevanza o stabilire determinate soglie limite, cosicché le banche siano tenute a segnalare i depositi di singoli clienti superiori a una certa quota percentuale del totale di bilancio. Sono tuttavia necessarie salvaguardie per assicurare che le informazioni su singoli conti vengano utilizzate esclusivamente per legittimi fini prudenziali e possano essere protette in modo soddisfacente da parte di chi li riceve. A questo riguardo, sarebbe utile un protocollo di mutua collaborazione¹⁸ per facilitare lo scambio di informazioni fra le autorità di vigilanza delle due giurisdizioni.

69. In certi casi può sussistere un serio conflitto fra le politiche KYC della casa madre imposte dall'autorità di vigilanza nazionale e le attività permesse a una sua dipendenza all'estero. Può accadere, ad esempio, che la legislazione locale non permetta ispezioni da parte dei responsabili del controllo di conformità, dei revisori interni o degli organi di vigilanza dell'istituzione madre, o consenta ai clienti di utilizzare nomi fittizi o di celarsi dietro rappresentanti o intermediari cui è fatto divieto di

¹⁸ Si veda il documento del Comitato di Basilea *Essential elements of a statement of cooperation between banking supervisors* (maggio 2001).

rivelare l'identità dei propri clienti. In tali casi l'autorità del paese d'origine dovrebbe comunicare con l'autorità del paese ospitante al fine di appurare se esistono effettivi impedimenti legali e se questi si applicano extra-territorialmente. Qualora gli ostacoli si rivelino insormontabili e non siano possibili alternative soddisfacenti, l'autorità del paese d'origine dovrebbe far chiaramente intendere alla sua omologa che la banca potrebbe decidere, autonomamente o su richiesta dell'autorità stessa, di chiudere la dipendenza in questione. In definitiva, qualsiasi accordo a sostegno di tali ispezioni in loco dovrebbe prevedere meccanismi atti a consentire una valutazione che sia soddisfacente per l'autorità del paese d'origine. A tale riguardo, possono essere utili dichiarazioni di cooperazione o protocolli d'intesa che stabiliscano i meccanismi di questi accordi. L'accesso alle informazioni da parte del paese d'origine dovrebbe essere il più possibile libero da restrizioni e permettere, come minimo, l'accertamento delle politiche e procedure generali della banca in relazione al dovere di diligenza nell'identificazione dei clienti e nel trattamento dei casi sospetti.

Allegato 1

Estratto dal documento *Metodologia dei Principi fondamentali per un'efficace vigilanza bancaria*

Principio 15: Le autorità di vigilanza bancaria devono poter accertare che le banche applicano politiche, prassi e procedure (compresi criteri rigorosi in merito alla conoscenza del cliente) tali da promuovere un elevato standard etico e professionale nel settore finanziario e da impedire che la banca si presti, con o senza intenzionalità, a essere utilizzata da elementi criminali.

Criteri essenziali

1. L'autorità di vigilanza accerta che le banche dispongano di adeguate politiche, prassi e procedure per promuovere un elevato standard etico e professionale e per impedire che la banca si presti, con o senza intenzionalità, a essere utilizzata da elementi criminali. Ne fanno parte la prevenzione e l'individuazione di attività criminose o frodi e la segnalazione di tali attività sospette alle autorità competenti.
2. L'autorità di vigilanza accerta che le banche dispongano, nel quadro dei programmi antiriciclaggio, di politiche documentate e applicate di fatto per l'identificazione dei clienti e dei soggetti che agiscono per loro conto. Esistono chiare regole che stabiliscono la documentazione da tenersi sull'identificazione del cliente e sulle singole transazioni, nonché il suo periodo di conservazione.
3. L'autorità di vigilanza accerta che le banche dispongano di procedure formali per l'individuazione delle transazioni potenzialmente sospette. Tali procedure possono prevedere autorizzazioni aggiuntive per i depositi e prelievi in contante (o simili) di grande ammontare e procedimenti speciali per le transazioni inusuali.
4. L'autorità di vigilanza accerta che le banche designino un alto funzionario avente la responsabilità esplicita di assicurare che le politiche e le procedure della banca siano come minimo conformi alle prescrizioni legali e regolamentari locali in materia di lotta al riciclaggio di capitali.
5. L'autorità di vigilanza accerta che le banche dispongano di procedure chiare, rese note a tutto il personale, per la segnalazione interna delle transazioni sospette al funzionario responsabile della conformità con la normativa antiriciclaggio.
6. L'autorità di vigilanza accerta che le banche abbiano istituito linee di comunicazione sia verso la direzione che verso la funzione di sicurezza interna per la segnalazione dei casi problematici.
7. Oltre a riferire alle competenti autorità giudiziarie, le banche segnalano alle autorità di vigilanza le attività sospette e gli atti di frode rilevanti ai fini della sicurezza, della solidità e della reputazione della banca.
8. Le leggi, i regolamenti e/o le politiche delle banche assicurano che i dipendenti i quali segnalano in buona fede transazioni sospette al dirigente preposto, alla funzione di sicurezza interna o direttamente all'autorità competente non possano essere ritenuti responsabili di violazione di obblighi.
9. L'autorità di vigilanza verifica periodicamente che i controlli antiriciclaggio delle banche e i loro sistemi per prevenire, individuare e segnalare le frodi siano sufficienti. L'autorità di vigilanza dispone di adeguati poteri coercitivi (promovimento di azione civile e/o penale) per agire nei confronti di una banca che non si conformi alle prescrizioni antiriciclaggio.
10. L'autorità di vigilanza è in grado, direttamente o indirettamente, di scambiare con altre istanze di controllo del settore finanziario nazionali o estere informazioni inerenti a presunte o effettive attività criminose.

11. L'autorità di vigilanza accerta che le banche abbiano adottato una dichiarazione di principi in materia di etica e comportamento professionali comunicata in termini chiari a tutto il personale.

Criteri integrativi

1. Le leggi e/o i regolamenti incorporano i principi internazionali per una corretta prassi, come le 40 Raccomandazioni della Financial Action Task Force (FATF/GAFI) emanate nel 1990 (rivedute nel 1996).
2. L'autorità di vigilanza accerta che il personale delle banche sia adeguatamente addestrato in materia di individuazione e prevenzione del riciclaggio di denaro.
3. L'autorità di vigilanza è tenuta per legge a segnalare alle competenti autorità penali ogni transazione sospetta.
4. L'autorità di vigilanza è in grado, direttamente o indirettamente, di scambiare con le competenti autorità giudiziarie informazioni inerenti a presunte o effettive attività criminali.
5. Ove la funzione non sia espletata da altro organo, l'autorità di vigilanza dispone di risorse interne con competenze specialistiche in materia di frode finanziaria e di prescrizioni antiriciclaggio.

Allegato 2

Estratto dalle Raccomandazioni FATF/GAFI

C. Ruolo del sistema finanziario nella lotta al riciclaggio dei fondi di provenienza illecita

Regole per l'identificazione dei clienti e la tenuta della documentazione

10. Le istituzioni finanziarie non dovrebbero intrattenere conti anonimi o intestati a nomi manifestamente fittizi: esse dovrebbero essere tenute (in forza di leggi, regolamenti, accordi fra le autorità di vigilanza e le istituzioni finanziarie o accordi di autoregolamentazione fra le istituzioni finanziarie) a identificare i clienti, sia occasionali che usuali, sulla base di un documento di riconoscimento ufficiale o di altro documento affidabile, e a registrarne le generalità, allorché stabiliscono relazioni d'affari o effettuano operazioni (in particolare, apertura di conti o depositi, esecuzione di transazioni fiduciarie, locazione di cassette di sicurezza, operazioni in contante di grande ammontare).

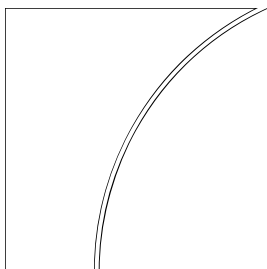
Al fine di adempiere i requisiti di identificazione concernenti le persone giuridiche, le istituzioni finanziarie dovrebbero, ove necessario, adottare misure per:

- (i) verificare l'esistenza e la struttura giuridica del cliente, ottenendo da un pubblico registro o dal cliente stesso, ovvero da entrambi, prova della costituzione in società, corredata di informazioni concernenti la ragione sociale, la forma giuridica, la sede, gli amministratori e le disposizioni che regolano la capacità di obbligare legalmente l'ente;
 - (ii) verificare se ogni persona che affermi di agire in nome del cliente sia a ciò autorizzata e identificare tale persona.
11. Le istituzioni finanziarie dovrebbero adottare misure ragionevoli per ottenere informazioni sulla vera identità delle persone in favore delle quali è aperto un conto o effettuata un'operazione se vi è ragione di dubitare che il cliente stia agendo per proprio conto, come ad esempio nel caso delle società di comodo (ossia istituzioni, società, fondazioni, trust, ecc. che non svolgono alcuna attività commerciale o industriale, né hanno altre forme di operatività nel paese in cui è situata la loro sede legale).
12. Le istituzioni finanziarie dovrebbero conservare per almeno cinque anni tutta la necessaria documentazione sulle operazioni compiute, sia nazionali che internazionali, affinché possano essere soddisfatte prontamente eventuali richieste di informazioni da parte delle autorità competenti. La documentazione deve essere sufficiente a permettere la ricostruzione delle singole operazioni (compresi gli importi e i tipi di moneta, se del caso) così da fornire, ove necessario, elementi di prova per il perseguimento di comportamenti delittuosi.
- Le istituzioni finanziarie dovrebbero conservare la documentazione relativa all'identificazione del cliente (ad esempio, copie o annotazioni dei documenti di riconoscimento ufficiali come passaporti, carte d'identità, patenti di guida o simili), i registri dei conti e la corrispondenza commerciale per almeno cinque anni dalla data di chiusura del conto.
- Questa documentazione dovrebbe essere a disposizione delle autorità nazionali competenti nel caso di procedimenti o istruttorie penali.
13. I paesi dovrebbero dedicare particolare attenzione ai pericoli di riciclaggio di capitali insiti nelle tecnologie nuove o in evoluzione idonee a favorire l'anonimato e dovrebbero, ove necessario, adottare provvedimenti per impedire il loro utilizzo come canali di riciclaggio.

Accresciuta diligenza delle istituzioni finanziarie

14. Le istituzioni finanziarie dovrebbero dedicare particolare attenzione a tutte le operazioni complesse e di ammontare insolitamente elevato, nonché a tutti i tipi di operazioni che non hanno una palese finalità economica o uno scopo legittimo visibile. Per quanto possibile, dovrebbero essere analizzati gli aspetti sottostanti e il fine di tali operazioni; i risultati dell'analisi dovrebbero essere documentati per iscritto e tenuti a disposizione delle autorità di vigilanza, dei revisori e degli organi giudiziari e di polizia.
15. Allorché le istituzioni finanziarie sospettano che i fondi provengano da un'attività criminale, esse dovrebbero essere tenute a segnalare prontamente tali sospetti alle autorità competenti.
16. Le istituzioni finanziarie e i loro amministratori, funzionari e dipendenti dovrebbero essere protetti in forza di legge da ogni responsabilità penale o civile per violazione dei vincoli di riservatezza – siano essi imposti per contratto o da disposizioni legali, regolamentari o amministrative – allorché segnalano in buona fede i propri sospetti alle autorità competenti, quand'anche non sappiano esattamente di quale fattispecie criminosa si tratti e prescindendo dal fatto che risulti esservi effettivamente stata un'attività illecita.
17. Le istituzioni finanziarie e i loro amministratori, funzionari e dipendenti non dovrebbero avvertire o, se del caso, essere autorizzati ad avvertire i clienti del fatto che informazioni che li riguardano sono state trasmesse alle autorità competenti.
18. Le istituzioni finanziarie che segnalano operazioni sospette dovrebbero conformarsi alle istruzioni delle autorità competenti.
19. Le istituzioni finanziarie dovrebbero porre in essere programmi contro il riciclaggio di denaro che prevedano come minimo:
 - (i) la definizione di politiche, procedure e controlli interni, ivi compresa la designazione di responsabili per il controllo di conformità a livello di direzione, e adeguate procedure di selezione per assicurare standard elevati in sede di assunzione del personale;
 - (ii) un programma continuativo di formazione del personale;
 - (iii) una funzione di audit per verificare il sistema.

Basel Committee
on Banking Supervision



**Customer due diligence
for banks**

October 2001

415

EBK Bulletin 44/2003



BANK FOR INTERNATIONAL SETTLEMENTS

Working Group on Cross-border Banking

Co-Chairs:

Mr Charles Freeland, Deputy Secretary General, Basel Committee on Banking Supervision

Mr Colin Powell, Chairman, Offshore Group of Banking Supervisors, and Chairman, Jersey Financial Services Commission

Bermuda Monetary Authority	Mr D Munro Sutherland
Cayman Islands Monetary Authority	Mr John Bourbon Mrs Anna McLean
Banque de France/Commission Bancaire	Mr Laurent Ettori
Federal Banking Supervisory Office of Germany	Mr Jochen Sanio Mr Peter Kruschel
Guernsey Financial Services Commission	Mr Peter G Crook (until April 2001) Mr Philip Marr (since April 2001)
Banca d'Italia	Mr Giuseppe Godano
Financial Services Agency, Japan	Mr Kiyotaka Sasaki (until July 2001) Mr Hisashi Ono (since July 2001)
Commission de Surveillance du Secteur Financier, Luxembourg	Mr Romain Strock
Monetary Authority of Singapore	Mrs Foo-Yap Siew Hong Ms Teo Lay Har
Swiss Federal Banking Commission	Mr Daniel Zuberbühler Ms Dina Balleyguier
Financial Services Authority, United Kingdom	Mr Richard Chalmers
Board of Governors of the Federal Reserve System	Mr William Ryback
Federal Reserve Bank of New York	Ms Nancy Bercovici
Office of the Comptroller of the Currency	Mr Jose Tuya Ms Tanya Smith
Secretariat	Mr Andrew Khoo

Table of Contents

I.	Introduction	2
II.	Importance of KYC standards for supervisors and banks	3
III.	Essential elements of KYC standards	5
1.	Customer acceptance policy	6
2.	Customer identification.....	6
2.1	General identification requirements.....	7
2.2	Specific identification issues	8
2.2.1	Trust, nominee and fiduciary accounts.....	8
2.2.2	Corporate vehicles.....	8
2.2.3	Introduced business.....	9
2.2.4	Client accounts opened by professional intermediaries.....	9
2.2.5	Politically exposed persons.....	10
2.2.6	Non-face-to-face customers.....	11
2.2.7	Correspondent banking.....	12
3.	On-going monitoring of accounts and transactions.....	13
4.	Risk management.....	14
IV.	The role of supervisors.....	14
V.	Implementation of KYC standards in a cross-border context	15
	Annex 1: Excerpts from <i>Core Principles Methodology</i>	18
	Annex 2: Excerpts from FATF recommendations	20

Customer due diligence for banks

I. Introduction

1. Supervisors around the world are increasingly recognising the importance of ensuring that their banks have adequate controls and procedures in place so that they know the customers with whom they are dealing. Adequate due diligence on new and existing customers is a key part of these controls. Without this due diligence, banks can become subject to reputational, operational, legal and concentration risks, which can result in significant financial cost.

2. In reviewing the findings of an internal survey of cross-border banking in 1999, the Basel Committee identified deficiencies in a large number of countries' know-your-customer (KYC) policies for banks. Judged from a supervisory perspective, KYC policies in some countries have significant gaps and in others they are non-existent. Even among countries with well-developed financial markets, the extent of KYC robustness varies. Consequently, the Basel Committee asked the Working Group on Cross-border Banking¹ to examine the KYC procedures currently in place and to draw up recommended standards applicable to banks in all countries. The resulting paper was issued as a consultative document in January 2001. Following a review of the comments received, the Working Group has revised the paper and the Basel Committee is now distributing it worldwide in the expectation that the KYC framework presented here will become the benchmark for supervisors to establish national practices and for banks to design their own programmes. It is important to acknowledge that supervisory practices of some jurisdictions already meet or exceed the objective of this paper and, as a result, they may not need to implement any changes.

3. KYC is most closely associated with the fight against money-laundering, which is essentially the province of the Financial Action Task Force (FATF).² It is not the Committee's intention to duplicate the efforts of the FATF. Instead, the Committee's interest is from a wider prudential perspective. Sound KYC policies and procedures are critical in protecting the safety and soundness of banks and the integrity of banking systems. The Basel Committee and the Offshore Group of Banking Supervisors (OGBS) continue to support strongly the adoption and implementation of the FATF recommendations, particularly those relating to banks, and intend the standards in this paper to be consistent with the FATF recommendations. The Committee and the OGBS will also consider the adoption of any higher standards introduced by the FATF as a result of its current review of the 40 Recommendations. Consequently, the Working Group has been and will remain in close contact with the FATF as it develops its thoughts.

4. The Basel Committee's approach to KYC is from a wider prudential, not just anti-money laundering, perspective. Sound KYC procedures must be seen as a critical element in the effective management of banking risks. KYC safeguards go beyond simple account

¹ This is a joint group consisting of members of the Basel Committee and of the Offshore Group of Banking Supervisors.

² The FATF is an inter-governmental body which develops and promotes policies, both nationally and internationally, to combat money laundering. It has 29 member countries and two regional organisations. It works in close cooperation with other international bodies involved in this area such as the United Nations Office for Drug Control and Crime Prevention, the Council of Europe, the Asia-Pacific Group on Money Laundering and the Caribbean Financial Action Task Force. The FATF defines money laundering as the processing of criminal proceeds in order to disguise their illegal origin.

opening and record-keeping and require banks to formulate a customer acceptance policy and a tiered customer identification programme that involves more extensive due diligence for higher risk accounts, and includes proactive account monitoring for suspicious activities.

5. The Basel Committee's interest in sound KYC standards originates from its concerns for market integrity and has been heightened by the direct and indirect losses incurred by banks due to their lack of diligence in applying appropriate procedures. These losses could probably have been avoided and damage to the banks' reputation significantly diminished had the banks maintained effective KYC programmes.

6. This paper reinforces the principles established in earlier Committee papers by providing more precise guidance on the essential elements of KYC standards and their implementation. In developing this guidance, the Working Group has drawn on practices in member countries and taken into account evolving supervisory developments. The essential elements presented in this paper are guidance as to minimum standards for worldwide implementation for all banks. These standards may need to be supplemented and/or strengthened, by additional measures tailored to the risks of particular institutions and risks in the banking system of individual countries. For example, enhanced diligence is required in the case of higher-risk accounts or for banks that specifically aim to attract high net-worth customers. In a number of specific sections in this paper, there are recommendations for higher standards of due diligence for higher risk areas within a bank, where applicable.

7. The need for rigorous customer due diligence standards is not restricted to banks. The Basel Committee believes similar guidance needs to be developed for all non-bank financial institutions and professional intermediaries of financial services such as lawyers and accountants.

II. Importance of KYC standards for supervisors and banks

8. The FATF and other international groupings have worked intensively on KYC issues, and the FATF's 40 Recommendations on combating money-laundering³ have international recognition and application. It is not the intention of this paper to duplicate that work.

9. At the same time, sound KYC procedures have particular relevance to the safety and soundness of banks, in that:

- they help to protect banks' reputation and the integrity of banking systems by reducing the likelihood of banks becoming a vehicle for or a victim of financial crime and suffering consequential reputational damage;
- they constitute an essential part of sound risk management (e.g. by providing the basis for identifying, limiting and controlling risk exposures in assets and liabilities, including assets under management).

10. The inadequacy or absence of KYC standards can subject banks to serious customer and counterparty risks, especially **reputational, operational, legal and concentration risks**. It is worth noting that all these risks are interrelated. However, any one

³ See FATF recommendations 10 to 19 which are reproduced in Annex 2.

of them can result in significant financial cost to banks (e.g. through the withdrawal of funds by depositors, the termination of inter-bank facilities, claims against the bank, investigation costs, asset seizures and freezes, and loan losses), as well as the need to divert considerable management time and energy to resolving problems that arise.

11. **Reputational risk** poses a major threat to banks, since the nature of their business requires maintaining the confidence of depositors, creditors and the general marketplace. Reputational risk is defined as the potential that adverse publicity regarding a bank's business practices and associations, whether accurate or not, will cause a loss of confidence in the integrity of the institution. Banks are especially vulnerable to reputational risk because they can so easily become a vehicle for or a victim of illegal activities perpetrated by their customers. They need to protect themselves by means of continuous vigilance through an effective KYC programme. Assets under management, or held on a fiduciary basis, can pose particular reputational dangers.

12. **Operational risk** can be defined as the risk of direct or indirect loss resulting from inadequate or failed internal processes, people and systems or from external events. Most operational risk in the KYC context relates to weaknesses in the implementation of banks' programmes, ineffective control procedures and failure to practise due diligence. A public perception that a bank is not able to manage its operational risk effectively can disrupt or adversely affect the business of the bank.

13. **Legal risk** is the possibility that lawsuits, adverse judgements or contracts that turn out to be unenforceable can disrupt or adversely affect the operations or condition of a bank. Banks may become subject to lawsuits resulting from the failure to observe mandatory KYC standards or from the failure to practise due diligence. Consequently, banks can, for example, suffer fines, criminal liabilities and special penalties imposed by supervisors. Indeed, a court case involving a bank may have far greater cost implications for its business than just the legal costs. Banks will be unable to protect themselves effectively from such legal risks if they do not engage in due diligence in identifying their customers and understanding their business.

14. Supervisory concern about **concentration risk** mostly applies on the assets side of the balance sheet. As a common practice, supervisors not only require banks to have information systems to identify credit concentrations but most also set prudential limits to restrict banks' exposures to single borrowers or groups of related borrowers. Without knowing precisely who the customers are, and their relationship with other customers, it will not be possible for a bank to measure its concentration risk. This is particularly relevant in the context of related counterparties and connected lending.

15. On the liabilities side, concentration risk is closely associated with funding risk, particularly the risk of early and sudden withdrawal of funds by large depositors, with potentially damaging consequences for the bank's liquidity. Funding risk is more likely to be higher in the case of small banks and those that are less active in the wholesale markets than large banks. Analysing deposit concentrations requires banks to understand the characteristics of their depositors, including not only their identities but also the extent to which their actions may be linked with those of other depositors. It is essential that liabilities managers in small banks not only know but maintain a close relationship with large depositors, or they will run the risk of losing their funds at critical times.

16. Customers frequently have multiple accounts with the same bank, but in offices located in different countries. To effectively manage the reputational, compliance and legal risk arising from such accounts, banks should be able to aggregate and monitor significant balances and activity in these accounts on a fully consolidated worldwide basis, regardless of

whether the accounts are held on balance sheet, off balance sheet, as assets under management, or on a fiduciary basis.

17. Both the Basel Committee and the Offshore Group of Banking Supervisors are fully convinced that effective KYC practices should be part of the risk management and internal control systems in all banks worldwide. National supervisors are responsible for ensuring that banks have minimum standards and internal controls that allow them to adequately know their customers. Voluntary codes of conduct⁴ issued by industry organisations or associations can be of considerable value in underpinning regulatory guidance, by giving practical advice to banks on operational matters. However, such codes cannot be regarded as a substitute for formal regulatory guidance.

III. Essential elements of KYC standards

18. The Basel Committee's guidance on KYC has been contained in the following three papers and they reflect the evolution of the supervisory thinking over time. *The Prevention of Criminal Use of the Banking System for the Purpose of Money-Laundering* issued in 1988 stipulates the basic ethical principles and encourages banks to put in place effective procedures to identify customers, decline suspicious transactions and cooperate with law enforcement agencies. The 1997 *Core Principles for Effective Banking Supervision* states, in a broader discussion of internal controls, that banks should have adequate policies, practices and procedures in place, including strict "know-your-customer" rules; specifically, supervisors should encourage the adoption of the relevant recommendations of the FATF. These relate to customer identification and record-keeping, increased diligence by financial institutions in detecting and reporting suspicious transactions, and measures to deal with countries with inadequate anti-money laundering measures. The 1999 *Core Principles Methodology* further elaborates the Core Principles by listing a number of essential and additional criteria. (Annex 1 sets out the relevant extracts from the *Core Principles* and the *Methodology*.)

19. All banks should be required to "have in place adequate policies, practices and procedures that promote high ethical and professional standards and prevent the bank from being used, intentionally or unintentionally, by criminal elements".⁵ Certain key elements should be included by banks in the design of KYC programmes. Such essential elements should start from the banks' risk management and control procedures and should include (1) customer acceptance policy, (2) customer identification, (3) on-going monitoring of high risk accounts and (4) risk management. Banks should not only establish the identity of their customers, but should also monitor account activity to determine those transactions that do not conform with the normal or expected transactions for that customer or type of account. KYC should be a core feature of banks' risk management and control procedures, and be complemented by regular compliance reviews and internal audit. The intensity of KYC programmes beyond these essential elements should be tailored to the degree of risk.

⁴ An example of an industry code is the "Global anti-money-laundering guidelines for Private Banking" (also called the Wolfsberg Principles) that was drawn up in October 2000 by twelve major banks with significant involvement in private banking.

⁵ *Core Principles Methodology*, Essential Criterion 1.

1. Customer acceptance policy

20. Banks should develop clear customer acceptance policies and procedures, including a description of the types of customer that are likely to pose a higher than average risk to a bank. In preparing such policies, factors such as customers' background, country of origin, public or high profile position, linked accounts, business activities or other risk indicators should be considered. Banks should develop graduated customer acceptance policies and procedures that require more extensive due diligence for higher risk customers. For example, the policies may require the most basic account-opening requirements for a working individual with a small account balance. It is important that the customer acceptance policy is not so restrictive that it results in a denial of access by the general public to banking services, especially for people who are financially or socially disadvantaged. On the other hand, quite extensive due diligence would be essential for an individual with a high net worth whose source of funds is unclear. Decisions to enter into business relationships with higher risk customers, such as politically exposed persons (see section 2.2.3 below), should be taken exclusively at senior management level.

2. Customer identification

21. Customer identification is an essential element of KYC standards. For the purposes of this paper, a customer includes:

- the person or entity that maintains an account with the bank or those on whose behalf an account is maintained (i.e. beneficial owners);
- the beneficiaries of transactions conducted by professional intermediaries; and
- any person or entity connected with a financial transaction who can pose a significant reputational or other risk to the bank.

22. Banks should establish a systematic procedure for identifying new customers and should not establish a banking relationship until the identity of a new customer is satisfactorily verified.

23. Banks should "document and enforce policies for identification of customers and those acting on their behalf".⁶ The best documents for verifying the identity of customers are those most difficult to obtain illicitly and to counterfeit. Special attention should be exercised in the case of non-resident customers and in no case should a bank short-circuit identity procedures just because the new customer is unable to present himself for interview. The bank should always ask itself why the customer has chosen to open an account in a foreign jurisdiction.

24. The customer identification process applies naturally at the outset of the relationship. To ensure that records remain up-to-date and relevant, there is a need for banks to undertake regular reviews of existing records.⁷ An appropriate time to do so is when a transaction of significance takes place, when customer documentation standards change substantially, or when there is a material change in the way that the account is operated. However, if a bank becomes aware at any time that it lacks sufficient information about an

⁶ *Core Principles Methodology*, Essential Criterion 2.

⁷ The application of new KYC standards to existing accounts is currently subject to FATF review.

existing customer, it should take steps to ensure that all relevant information is obtained as quickly as possible.

25. Banks that offer private banking services are particularly exposed to reputational risk, and should therefore apply enhanced due diligence to such operations. Private banking accounts, which by nature involve a large measure of confidentiality, can be opened in the name of an individual, a commercial business, a trust, an intermediary or a personalised investment company. In each case reputational risk may arise if the bank does not diligently follow established KYC procedures. All new clients and new accounts should be approved by at least one person, of appropriate seniority, other than the private banking relationship manager. If particular safeguards are put in place internally to protect confidentiality of private banking customers and their business, banks must still ensure that at least equivalent scrutiny and monitoring of these customers and their business can be conducted, e.g. they must be open to review by compliance officers and auditors.

26. Banks should develop "clear standards on what records must be kept on customer identification and individual transactions and their retention period".⁸ Such a practice is essential to permit a bank to monitor its relationship with the customer, to understand the customer's on-going business and, if necessary, to provide evidence in the event of disputes, legal action, or a financial investigation that could lead to criminal prosecution. As the starting point and natural follow-up of the identification process, banks should obtain customer identification papers and retain copies of them for at least five years after an account is closed. They should also retain all financial transaction records for at least five years after the transaction has taken place.

2.1 General identification requirements

27. Banks need to obtain all information necessary to establish to their full satisfaction the identity of each new customer and the purpose and intended nature of the business relationship. The extent and nature of the information depends on the type of applicant (personal, corporate, etc.) and the expected size of the account. National supervisors are encouraged to provide guidance to assist banks in designing their own identification procedures. The Working Group intends to develop essential elements of customer identification requirements.

28. When an account has been opened, but problems of verification arise in the banking relationship which cannot be resolved, the bank should close the account and return the monies to the source from which they were received.⁹

29. While the transfer of an opening balance from an account in the customer's name in another bank subject to the same KYC standard may provide some comfort, banks should nevertheless consider the possibility that the previous account manager may have asked for the account to be removed because of a concern about dubious activities. Naturally, customers have the right to move their business from one bank to another. However, if a bank has any reason to believe that an applicant is being refused banking facilities by another bank, it should apply enhanced diligence procedures to the customer.

⁸ *Core Principles Methodology*, Essential Criterion 2.

⁹ Subject to any national legislation concerning handling of suspicious transactions.

30. Banks should never agree to open an account or conduct ongoing business with a customer who insists on anonymity or who gives a fictitious name. Nor should confidential numbered¹⁰ accounts function as anonymous accounts but they should be subject to exactly the same KYC procedures as all other customer accounts, even if the test is carried out by selected staff. Whereas a numbered account can offer additional protection for the identity of the account-holder, the identity must be known to a sufficient number of staff to operate proper due diligence. Such accounts should in no circumstances be used to hide the customer identity from a bank's compliance function or from the supervisors.

2.2 Specific identification issues

31. There are a number of more detailed issues relating to customer identification which need to be addressed. Several of these are currently under consideration by the FATF as part of a general review of its 40 recommendations, and the Working Group recognises the need to be consistent with the FATF.

2.2.1 Trust, nominee and fiduciary accounts

32. Trust, nominee and fiduciary accounts can be used to circumvent customer identification procedures. While it may be legitimate under certain circumstances to provide an extra layer of security to protect the confidentiality of legitimate private banking customers, it is essential that the true relationship is understood. Banks should establish whether the customer is taking the name of another customer, acting as a "front", or acting on behalf of another person as trustee, nominee or other intermediary. If so, a necessary precondition is receipt of satisfactory evidence of the identity of any intermediaries, and of the persons upon whose behalf they are acting, as well as details of the nature of the trust or other arrangements in place. Specifically, the identification of a trust should include the trustees, settlors/grantors and beneficiaries.¹¹

2.2.2 Corporate vehicles

33. Banks need to be vigilant in preventing corporate business entities from being used by natural persons as a method of operating anonymous accounts. Personal asset holding vehicles, such as international business companies, may make proper identification of customers or beneficial owners difficult. A bank should understand the structure of the company, determine the source of funds, and identify the beneficial owners and those who have control over the funds.

34. Special care needs to be exercised in initiating business transactions with companies that have nominee shareholders or shares in bearer form. Satisfactory evidence of the identity of beneficial owners of all such companies needs to be obtained. In the case of entities which have a significant proportion of capital in the form of bearer shares, extra vigilance is called for. A bank may be completely unaware that the bearer shares have changed hands. The onus is on banks to put in place satisfactory procedures to monitor the

¹⁰ In a numbered account, the name of the beneficial owner is known to the bank but is substituted by an account number or code name in subsequent documentation.

¹¹ Beneficiaries should be identified as far as possible when defined. It is recognised that it may not be possible to identify the beneficiaries of trusts precisely at the outset. For example, some beneficiaries may be unborn children and some may be conditional on the occurrence of specific events. In addition, beneficiaries being specific classes of individuals (e.g. employee pension funds) may be appropriately dealt with as pooled accounts as referred to in paragraphs 38-9.

identity of material beneficial owners. This may require the bank to immobilise the shares, e.g. by holding the bearer shares in custody.

2.2.3 *Introduced business*

35. The performance of identification procedures can be time consuming and there is a natural desire to limit any inconvenience for new customers. In some countries, it has therefore become customary for banks to rely on the procedures undertaken by other banks or introducers when business is being referred. In doing so, banks risk placing excessive reliance on the due diligence procedures that they expect the introducers to have performed. Relying on due diligence conducted by an introducer, however reputable, does not in any way remove the ultimate responsibility of the recipient bank to know its customers and their business. In particular, banks should not rely on introducers that are subject to weaker standards than those governing the banks' own KYC procedures or that are unwilling to share copies of due diligence documentation.

36. The Basel Committee recommends that banks that use introducers should carefully assess whether the introducers are "fit and proper" and are exercising the necessary due diligence in accordance with the standards set out in this paper. The ultimate responsibility for knowing customers always lies with the bank. Banks should use the following criteria to determine whether an introducer can be relied upon:¹²

- it must comply with the minimum customer due diligence practices identified in this paper;
- the customer due diligence procedures of the introducer should be as rigorous as those which the bank would have conducted itself for the customer;
- the bank must satisfy itself as to the reliability of the systems put in place by the introducer to verify the identity of the customer;
- the bank must reach agreement with the introducer that it will be permitted to verify the due diligence undertaken by the introducer at any stage; and
- all relevant identification data and other documentation pertaining to the customer's identity should be immediately submitted by the introducer to the bank, who must carefully review the documentation provided. Such information must be available for review by the supervisor and the financial intelligence unit or equivalent enforcement agency, where appropriate legal authority has been obtained.

In addition, banks should conduct periodic reviews to ensure that an introducer which it relies on continues to conform to the criteria set out above.

2.2.4 *Client accounts opened by professional intermediaries*

37. When a bank has knowledge or reason to believe that a client account opened by a professional intermediary is on behalf of a single client, that client must be identified.

38. Banks often hold "pooled" accounts managed by professional intermediaries on behalf of entities such as mutual funds, pension funds and money funds. Banks also hold

¹² The FATF is currently engaged in a review of the appropriateness of eligible introducers.

pooled accounts managed by lawyers or stockbrokers that represent funds held on deposit or in escrow for a range of clients. Where funds held by the intermediary are not co-mingled at the bank, but where there are "sub-accounts" which can be attributable to each beneficial owner, all beneficial owners of the account held by the intermediary must be identified.

39. Where the funds are co-mingled, the bank should look through to the beneficial owners. There can be circumstances where the bank may not need to look beyond the intermediary, for example, when the intermediary is subject to the same regulatory and money laundering legislation and procedures, and in particular is subject to the same due diligence standards in respect of its client base as the bank. National supervisory guidance should clearly set out those circumstances in which banks need not look beyond the intermediary. Banks should accept such accounts only on the condition that they are able to establish that the intermediary has engaged in a sound due diligence process and has the systems and controls to allocate the assets in the pooled accounts to the relevant beneficiaries. In assessing the due diligence process of the intermediary, the bank should apply the criteria set out in paragraph 36 above, in respect of introduced business, in order to determine whether a professional intermediary can be relied upon.

40. Where the intermediary is not empowered to furnish the required information on beneficiaries to the bank, for example, lawyers¹³ bound by professional secrecy codes or when that intermediary is not subject to due diligence standards equivalent to those set out in this paper or to the requirements of comprehensive anti-money laundering legislation, then the bank should not permit the intermediary to open an account.

2.2.5 *Politically exposed persons*

41. Business relationships with individuals holding important public positions and with persons or companies clearly related to them may expose a bank to significant reputational and/or legal risks. Such politically exposed persons ("PEPs") are individuals who are or have been entrusted with prominent public functions, including heads of state or of government, senior politicians, senior government, judicial or military officials, senior executives of publicly owned corporations and important political party officials. There is always a possibility, especially in countries where corruption is widespread, that such persons abuse their public powers for their own illicit enrichment through the receipt of bribes, embezzlement, etc.

42. Accepting and managing funds from corrupt PEPs will severely damage the bank's own reputation and can undermine public confidence in the ethical standards of an entire financial centre, since such cases usually receive extensive media attention and strong political reaction, even if the illegal origin of the assets is often difficult to prove. In addition, the bank may be subject to costly information requests and seizure orders from law enforcement or judicial authorities (including international mutual assistance procedures in criminal matters) and could be liable to actions for damages by the state concerned or the victims of a regime. Under certain circumstances, the bank and/or its officers and employees themselves can be exposed to charges of money laundering, if they know or should have known that the funds stemmed from corruption or other serious crimes.

43. Some countries have recently amended or are in the process of amending their laws and regulations to criminalise active corruption of foreign civil servants and public officers in

¹³ The FATF is currently engaged in a review of KYC procedures governing accounts opened by lawyers on behalf of clients.

accordance with the relevant international convention.¹⁴ In these jurisdictions foreign corruption becomes a predicate offence for money laundering and all the relevant anti-money laundering laws and regulations apply (e.g. reporting of suspicious transactions, prohibition on informing the customer, internal freeze of funds etc). But even in the absence of such an explicit legal basis in criminal law, it is clearly undesirable, unethical and incompatible with the fit and proper conduct of banking operations to accept or maintain a business relationship if the bank knows or must assume that the funds derive from corruption or misuse of public assets. There is a compelling need for a bank considering a relationship with a person whom it suspects of being a PEP to identify that person fully, as well as people and companies that are clearly related to him/her.

44. Banks should gather sufficient information from a new customer, and check publicly available information, in order to establish whether or not the customer is a PEP. Banks should investigate the source of funds before accepting a PEP. The decision to open an account for a PEP should be taken at a senior management level.

2.2.6 Non-face-to-face customers

45. Banks are increasingly asked to open accounts on behalf of customers who do not present themselves for personal interview. This has always been a frequent event in the case of non-resident customers, but it has increased significantly with the recent expansion of postal, telephone and electronic banking. Banks should apply equally effective customer identification procedures and on-going monitoring standards for non-face-to-face customers as for those available for interview. One issue that has arisen in this connection is the possibility of independent verification by a reputable third party. This whole subject of non-face-to-face customer identification is being discussed by the FATF, and is also under review in the context of amending the 1991 EEC Directive.

46. A typical example of a non-face-to-face customer is one who wishes to conduct electronic banking via the Internet or similar technology. Electronic banking currently incorporates a wide array of products and services delivered over telecommunications networks. The impersonal and borderless nature of electronic banking combined with the speed of the transaction inevitably creates difficulty in customer identification and verification. As a basic policy, supervisors expect that banks should proactively assess various risks posed by emerging technologies and design customer identification procedures with due regard to such risks.¹⁵

47. Even though the same documentation can be provided by face-to-face and non-face-to-face customers, there is a greater difficulty in matching the customer with the documentation in the case of non-face-to-face customers. With telephone and electronic banking, the verification problem is made even more difficult.

48. In accepting business from non-face-to-face customers:

- banks should apply equally effective customer identification procedures for non-face-to-face customers as for those available for interview; and

¹⁴ See OECD Convention on *Combating Bribery of Foreign Public Officials in International Business Transactions*, adopted by the Negotiating Conference on 21 November 1997.

¹⁵ The Electronic Banking Group of the Basel Committee issued a paper on risk management principles for electronic banking in May 2001.

- there must be specific and adequate measures to mitigate the higher risk.

Examples of measures to mitigate risk include:

- certification of documents presented;
- requisition of additional documents to complement those which are required for face-to-face customers;
- independent contact with the customer by the bank;
- third party introduction, e.g. by an introducer subject to the criteria established in paragraph 36; or
- requiring the first payment to be carried out through an account in the customer's name with another bank subject to similar customer due diligence standards.

2.2.7 Correspondent banking

49. Correspondent banking is the provision of banking services by one bank (the "correspondent bank") to another bank (the "respondent bank"). Used by banks throughout the world, correspondent accounts enable banks to conduct business and provide services that the banks do not offer directly. Correspondent accounts that merit particular care involve the provision of services in jurisdictions where the respondent banks have no physical presence. However, if banks fail to apply an appropriate level of due diligence to such accounts, they expose themselves to the range of risks identified earlier in this paper, and may find themselves holding and/or transmitting money linked to corruption, fraud or other illegal activity.

50. Banks should gather sufficient information about their respondent banks to understand fully the nature of the respondent's business. Factors to consider include: information about the respondent bank's management, major business activities, where they are located and its money-laundering prevention and detection efforts; the purpose of the account; the identity of any third party entities that will use the correspondent banking services; and the condition of bank regulation and supervision in the respondent's country. Banks should only establish correspondent relationships with foreign banks that are effectively supervised by the relevant authorities. For their part, respondent banks should have effective customer acceptance and KYC policies.

51. In particular, banks should refuse to enter into or continue a correspondent banking relationship with a bank incorporated in a jurisdiction in which it has no physical presence and which is unaffiliated with a regulated financial group (i.e. shell banks). Banks should pay particular attention when continuing relationships with respondent banks located in jurisdictions that have poor KYC standards or have been identified as being "non-cooperative" in the fight against anti-money laundering. Banks should establish that their respondent banks have due diligence standards as set out in this paper, and employ enhanced due diligence procedures with respect to transactions carried out through the correspondent accounts.

52. Banks should be particularly alert to the risk that correspondent accounts might be used directly by third parties to transact business on their own behalf (e.g. payable-through accounts). Such arrangements give rise to most of the same considerations applicable to introduced business and should be treated in accordance with the criteria set out in paragraph 36.

3. On-going monitoring of accounts and transactions

53. On-going monitoring is an essential aspect of effective KYC procedures. Banks can only effectively control and reduce their risk if they have an understanding of normal and reasonable account activity of their customers so that they have a means of identifying transactions which fall outside the regular pattern of an account's activity. Without such knowledge, they are likely to fail in their duty to report suspicious transactions to the appropriate authorities in cases where they are required to do so. The extent of the monitoring needs to be risk-sensitive. For all accounts, banks should have systems in place to detect unusual or suspicious patterns of activity. This can be done by establishing limits for a particular class or category of accounts. Particular attention should be paid to transactions that exceed these limits. Certain types of transactions should alert banks to the possibility that the customer is conducting unusual or suspicious activities. They may include transactions that do not appear to make economic or commercial sense, or that involve large amounts of cash deposits that are not consistent with the normal and expected transactions of the customer. Very high account turnover, inconsistent with the size of the balance, may indicate that funds are being "washed" through the account. Examples of suspicious activities can be very helpful to banks and should be included as part of a jurisdiction's anti-money-laundering procedures and/or guidance.

54. There should be intensified monitoring for higher risk accounts. Every bank should set key indicators for such accounts, taking note of the background of the customer, such as the country of origin and source of funds, the type of transactions involved, and other risk factors. For higher risk accounts:

- Banks should ensure that they have adequate management information systems to provide managers and compliance officers with timely information needed to identify, analyse and effectively monitor higher risk customer accounts. The types of reports that may be needed include reports of missing account opening documentation, transactions made through a customer account that are unusual, and aggregations of a customer's total relationship with the bank.
- Senior management in charge of private banking business should know the personal circumstances of the bank's high risk customers and be alert to sources of third party information. Significant transactions by these customers should be approved by a senior manager.
- Banks should develop a clear policy and internal guidelines, procedures and controls and remain especially vigilant regarding business relationships with PEPs and high profile individuals or with persons and companies that are clearly related to or associated with them.¹⁶ As all PEPs may not be identified initially and since existing customers may subsequently acquire PEP status, regular reviews of at least the more important customers should be undertaken.

¹⁶ It is unrealistic to expect the bank to know or investigate every distant family, political or business connection of a foreign customer. The need to pursue suspicions will depend on the size of the assets or turnover, pattern of transactions, economic background, reputation of the country, plausibility of the customer's explanations etc. It should however be noted that PEPs (or rather their family members and friends) would not necessarily present themselves in that capacity, but rather as ordinary (albeit wealthy) business people, masking the fact they owe their high position in a legitimate business corporation only to their privileged relation with the holder of the public office.

4. Risk management

55. Effective KYC procedures embrace routines for proper management oversight, systems and controls, segregation of duties, training and other related policies. The board of directors of the bank should be fully committed to an effective KYC programme by establishing appropriate procedures and ensuring their effectiveness. Explicit responsibility should be allocated within the bank for ensuring that the bank's policies and procedures are managed effectively and are, at a minimum, in accordance with local supervisory practice. The channels for reporting suspicious transactions should be clearly specified in writing, and communicated to all personnel. There should also be internal procedures for assessing whether the bank's statutory obligations under recognised suspicious activity reporting regimes require the transaction to be reported to the appropriate law enforcement and and/or supervisory authorities.

56. Banks' internal audit and compliance functions have important responsibilities in evaluating and ensuring adherence to KYC policies and procedures. As a general rule, the compliance function should provide an independent evaluation of the bank's own policies and procedures, including legal and regulatory requirements. Its responsibilities should include ongoing monitoring of staff performance through sample testing of compliance and review of exception reports to alert senior management or the Board of Directors if it believes management is failing to address KYC procedures in a responsible manner.

57. Internal audit plays an important role in independently evaluating the risk management and controls, discharging its responsibility to the Audit Committee of the Board of Directors or a similar oversight body through periodic evaluations of the effectiveness of compliance with KYC policies and procedures, including related staff training. Management should ensure that audit functions are staffed adequately with individuals who are well-versed in such policies and procedures. In addition, internal auditors should be proactive in following-up their findings and criticisms.

58. All banks must have an ongoing employee-training programme so that bank staff are adequately trained in KYC procedures. The timing and content of training for various sectors of staff will need to be adapted by the bank for its own needs. Training requirements should have a different focus for new staff, front-line staff, compliance staff or staff dealing with new customers. New staff should be educated in the importance of KYC policies and the basic requirements at the bank. Front-line staff members who deal directly with the public should be trained to verify the identity of new customers, to exercise due diligence in handling accounts of existing customers on an ongoing basis and to detect patterns of suspicious activity. Regular refresher training should be provided to ensure that staff are reminded of their responsibilities and are kept informed of new developments. It is crucial that all relevant staff fully understand the need for and implement KYC policies consistently. A culture within banks that promotes such understanding is the key to successful implementation.

59. In many countries, external auditors also have an important role to play in monitoring banks' internal controls and procedures, and in confirming that they are in compliance with supervisory practice.

IV. The role of supervisors

60. Based on existing international KYC standards, national supervisors are expected to set out supervisory practice governing banks' KYC programmes. The essential elements as

presented in this paper should provide clear guidance for supervisors to proceed with the work of designing or improving national supervisory practice.

61. In addition to setting out the basic elements for banks to follow, supervisors have a responsibility to monitor that banks are applying sound KYC procedures and are sustaining ethical and professional standards on a continuous basis. Supervisors should ensure that appropriate internal controls are in place and that banks are in compliance with supervisory and regulatory guidance. The supervisory process should include not only a review of policies and procedures but also a review of customer files and the sampling of some accounts. Supervisors should always have the right to access all documentation related to accounts maintained in that jurisdiction, including any analysis the bank has made to detect unusual or suspicious transactions.

62. Supervisors have a duty not only to ensure their banks maintain high KYC standards to protect their own safety and soundness but also to protect the integrity of their national banking system.¹⁷ Supervisors should make it clear that they will take appropriate action, which may be severe and public if the circumstances warrant, against banks and their officers who demonstrably fail to follow their own internal procedures and regulatory requirements. In addition, supervisors should ensure that banks are aware of and pay particular attention to transactions that involve jurisdictions where standards are considered inadequate. The FATF and some national authorities have listed a number of countries and jurisdictions that are considered to have legal and administrative arrangements that do not comply with international standards for combating money laundering. Such findings should be a component of a bank's KYC policies and procedures.

V. Implementation of KYC standards in a cross-border context

63. Supervisors around the world should seek, to the best of their efforts, to develop and implement their national KYC standards fully in line with international standards so as to avoid potential regulatory arbitrage and safeguard the integrity of domestic and international banking systems. The implementation and assessment of such standards put to the test the willingness of supervisors to cooperate with each other in a very practical way, as well as the ability of banks to control risks on a groupwide basis. This is a challenging task for banks and supervisors alike.

64. Supervisors expect banking groups to apply an accepted minimum standard of KYC policies and procedures to both their local and overseas operations. The supervision of international banking can only be effectively carried out on a consolidated basis, and reputational risk as well as other banking risks are not limited to national boundaries. Parent banks must communicate their policies and procedures to their overseas branches and subsidiaries, including non-banking entities such as trust companies, and have a routine for testing compliance against both home and host country KYC standards in order for their programmes to operate effectively globally. Such compliance tests will also be tested by external auditors and supervisors. Therefore, it is important that KYC documentation is properly filed and available for their inspection. As far as compliance checks are concerned, supervisors and external auditors should in most cases examine systems and controls and look at customer accounts and transactions monitoring as part of a sampling process.

¹⁷ Many supervisors also have a duty to report any suspicious, unusual or illegal transactions that they detect, for example, during onsite examinations.

65. However small an overseas establishment is, a senior officer should be designated to be directly responsible for ensuring that all relevant staff are trained in, and observe, KYC procedures that meet both home and host standards. While this officer will bear primary responsibility, he should be supported by internal auditors and compliance officers from both local and head offices as appropriate.

66. Where the minimum KYC standards of the home and host countries differ, branches and subsidiaries in the host jurisdictions should apply the higher standard of the two. In general, there should be no impediment to prevent a bank from adopting standards that are higher than the minima required locally. If, however, local laws and regulations (especially secrecy provisions) prohibit the implementation of home country KYC standards, where the latter are more stringent, host country supervisors should use their best endeavours to have the law and regulations changed. In the meantime, overseas branches and subsidiaries would have to comply with host country standards, but they should make sure the head office or parent bank and its home country supervisor are fully informed of the nature of the difference.

67. Criminal elements are likely to be drawn toward jurisdictions with such impediments. Hence, banks should be aware of the high reputational risk of conducting business in these jurisdictions. Parent banks should have a procedure for reviewing the vulnerability of the individual operating units and implement additional safeguards where appropriate. In extreme cases, supervisors should consider placing additional controls on banks operating in those jurisdictions and ultimately perhaps encouraging their withdrawal.

68. During on-site inspections, home country supervisors or auditors should face no impediments in verifying the unit's compliance with KYC policies and procedures. This will require a review of customer files and some random sampling of accounts. Home country supervisors should have access to information on sampled individual customer accounts to the extent necessary to enable a proper evaluation of the application of KYC standards and an assessment of risk management practices, and should not be impeded by local bank secrecy laws. Where the home country supervisor requires consolidated reporting of deposit or borrower concentrations or notification of funds under management, there should be no impediments. In addition, with a view to monitoring deposit concentrations or the funding risk of the deposit being withdrawn, home supervisors may apply materiality tests and establish some thresholds so that if a customer's deposit exceeds a certain percentage of the balance sheet, banks should report it to the home supervisor. However, safeguards are needed to ensure that information regarding individual accounts is used exclusively for lawful supervisory purposes, and can be protected by the recipient in a satisfactory manner. A statement of mutual cooperation¹⁸ to facilitate information sharing between the two supervisors would be helpful in this regard.

69. In certain cases there may be a serious conflict between the KYC policies of a parent bank imposed by its home authority and what is permitted in a cross-border office. There may, for example, be local laws that prevent inspections by the parent banks' compliance officers, internal auditors or home country supervisors, or that enable bank customers to use fictitious names or to hide behind agents or intermediaries that are forbidden from revealing who their clients are. In such cases, the home supervisor should communicate with the host supervisor in order to confirm whether there are indeed genuine legal impediments and whether they apply extraterritorially. If they prove to be

¹⁸ See the Basel Committee paper *Essential elements of a statement of cooperation between banking supervisors* (May 2001).

insurmountable, and there are no satisfactory alternative arrangements, the home supervisor should make it clear to the host that the bank may decide for itself, or be required by its home supervisor, to close down the operation in question. In the final analysis, any arrangements underpinning such on-site examinations should provide a mechanism that permits an assessment that is satisfactory to the home supervisor. Statements of cooperation or memoranda of understanding setting out the mechanics of the arrangements may be helpful. Access to information by home country supervisors should be as unrestricted as possible, and at a minimum they should have free access to the banks' general policies and procedures for customer due diligence and for dealing with suspicions.

Annex 1

Excerpts from *Core Principles Methodology*

Principle 15: Banking supervisors must determine that banks have adequate policies, practices and procedures in place, including strict “know-your-customer” rules, that promote high ethical and professional standards in the financial sector and prevent the bank being used, intentionally or unintentionally, by criminal elements.

Essential criteria

1. The supervisor determines that banks have in place adequate policies, practices and procedures that promote high ethical and professional standards and prevent the bank from being used, intentionally or unintentionally, by criminal elements. This includes the prevention and detection of criminal activity or fraud, and reporting of such suspected activities to the appropriate authorities.
2. The supervisor determines that banks have documented and enforced policies for identification of customers and those acting on their behalf as part of their anti-money-laundering program. There are clear rules on what records must be kept on customer identification and individual transactions and the retention period.
3. The supervisor determines that banks have formal procedures to recognise potentially suspicious transactions. These might include additional authorisation for large cash (or similar) deposits or withdrawals and special procedures for unusual transactions.
4. The supervisor determines that banks appoint a senior officer with explicit responsibility for ensuring that the bank's policies and procedures are, at a minimum, in accordance with local statutory and regulatory anti-money laundering requirements.
5. The supervisor determines that banks have clear procedures, communicated to all personnel, for staff to report suspicious transactions to the dedicated senior officer responsible for anti-money laundering compliance.
6. The supervisor determines that banks have established lines of communication both to management and to an internal security (guardian) function for reporting problems.
7. In addition to reporting to the appropriate criminal authorities, banks report to the supervisor suspicious activities and incidents of fraud material to the safety, soundness or reputation of the bank.
8. Laws, regulations and/or banks' policies ensure that a member of staff who reports suspicious transactions in good faith to the dedicated senior officer, internal security function, or directly to the relevant authority cannot be held liable.
9. The supervisor periodically checks that banks' money laundering controls and their systems for preventing, identifying and reporting fraud are sufficient. The supervisor has adequate enforcement powers (regulatory and/or criminal prosecution) to take

action against a bank that does not comply with its anti-money laundering obligations.

10. The supervisor is able, directly or indirectly, to share with domestic and foreign financial sector supervisory authorities information related to suspected or actual criminal activities.
11. The supervisor determines that banks have a policy statement on ethics and professional behaviour that is clearly communicated to all staff.

Additional criteria

1. The laws and/or regulations embody international sound practices, such as compliance with the relevant forty Financial Action Task Force Recommendations issued in 1990 (revised 1996).
2. The supervisor determines that bank staff is adequately trained on money laundering detection and prevention.
3. The supervisor has the legal obligation to inform the relevant criminal authorities of any suspicious transactions.
4. The supervisor is able, directly or indirectly, to share with relevant judicial authorities information related to suspected or actual criminal activities.
5. If not performed by another agency, the supervisor has in-house resources with specialist expertise on financial fraud and anti-money laundering obligations.

Annex 2

Excerpts from FATF recommendations

C. Role of the financial system in combating money laundering

Customer Identification and Record-keeping Rules

10. Financial institutions should not keep anonymous accounts or accounts in obviously fictitious names: they should be required (by law, by regulations, by agreements between supervisory authorities and financial institutions or by self-regulatory agreements among financial institutions) to identify, on the basis of an official or other reliable identifying document, and record the identity of their clients, either occasional or usual, when establishing business relations or conducting transactions (in particular opening of accounts or passbooks, entering into fiduciary transactions, renting of safe deposit boxes, performing large cash transactions).

In order to fulfil identification requirements concerning legal entities, financial institutions should, when necessary, take measures:

- (i) to verify the legal existence and structure of the customer by obtaining either from a public register or from the customer or both, proof of incorporation, including information concerning the customer's name, legal form, address, directors and provisions regulating the power to bind the entity.
 - (ii) to verify that any person purporting to act on behalf of the customer is so authorised and identify that person.
11. Financial institutions should take reasonable measures to obtain information about the true identity of the persons on whose behalf an account is opened or a transaction conducted if there are any doubts as to whether these clients or customers are acting on their own behalf, for example, in the case of domiciliary companies (i.e. institutions, corporations, foundations, trusts, etc. that do not conduct any commercial or manufacturing business or any other form of commercial operation in the country where their registered office is located).
12. Financial institutions should maintain, for at least five years, all necessary records on transactions, both domestic or international, to enable them to comply swiftly with information requests from the competent authorities. Such records must be sufficient to permit reconstruction of individual transactions (including the amounts and types of currency involved if any) so as to provide, if necessary, evidence for prosecution of criminal behaviour.

Financial institutions should keep records on customer identification (e.g. copies or records of official identification documents like passports, identity cards, driving licenses or similar documents), account files and business correspondence for at least five years after the account is closed.

These documents should be available to domestic competent authorities in the context of relevant criminal prosecutions and investigations.

13. Countries should pay special attention to money laundering threats inherent in new or developing technologies that might favour anonymity, and take measures, if needed, to prevent their use in money laundering schemes.

Increased Diligence of Financial Institutions

14. Financial institutions should pay special attention to all complex, unusual large transactions, and all unusual patterns of transactions, which have no apparent economic or visible lawful purpose. The background and purpose of such transactions should, as far as possible, be examined, the findings established in writing, and be available to help supervisors, auditors and law enforcement agencies.
15. If financial institutions suspect that funds stem from a criminal activity, they should be required to report promptly their suspicions to the competent authorities.
16. Financial institutions, their directors, officers and employees should be protected by legal provisions from criminal or civil liability for breach of any restriction on disclosure of information imposed by contract or by any legislative, regulatory or administrative provision, if they report their suspicions in good faith to the competent authorities, even if they did not know precisely what the underlying criminal activity was, and regardless of whether illegal activity actually occurred.
17. Financial institutions, their directors, officers and employees, should not, or, where appropriate, should not be allowed to, warn their customers when information relating to them is being reported to the competent authorities.
18. Financial institutions reporting their suspicions should comply with instructions from the competent authorities.
19. Financial institutions should develop programs against money laundering. These programs should include, as a minimum:
 - (i) the development of internal policies, procedures and controls, including the designation of compliance officers at management level, and adequate screening procedures to ensure high standards when hiring employees;
 - (ii) an ongoing employee training programme;
 - (iii) an audit function to test the system.

General Guide to Account Opening and Customer Identification

1. The Basel Committee on Banking Supervision in its paper on *Customer Due Diligence* for Banks published in October 2001 referred to the intention of the Working Group on Cross-border Banking¹ to develop guidance on customer identification. Customer identification is an essential element of an effective customer due diligence programme which banks need to put in place to guard against reputational, operational, legal and concentration risks. It is also necessary in order to comply with anti-money laundering legal requirements and a prerequisite for the identification of bank accounts related to terrorism.

2. What follows is account opening and customer identification guidelines and a general guide to good practice based on the principles of the Basel Committee's *Customer due diligence for banks* paper. This document, which has been developed by the Working Group on Cross-border Banking, does not cover every eventuality, but instead focuses on some of the mechanisms that banks can use in developing an effective customer identification programme.

3. These guidelines represent a starting point for supervisors and banks in the area of customer identification. This document does not address the other elements of the *Customer Due Diligence for banks* paper, such as the ongoing monitoring of accounts. However, these elements should be considered in the development of effective cus-

¹ The Working Group on Cross-border Banking is a joint group consisting of members of the Basel Committee and of the Offshore Group of Banking Supervisors.

tomer due diligence, anti-money laundering and combating the financing of terrorism procedures.

4. These guidelines may be adapted for use by national supervisors who are seeking to develop or enhance customer identification programmes. However, supervisors should recognize that any customer identification programme should reflect the different types of customers (individual vs. institution) and the different levels of risk resulting from a customer's relationship with a bank. Higher risk transactions and relationships, such as those with politically exposed persons or organisations, will clearly require greater scrutiny than lower risk transactions and accounts.

5. Guidelines and best practices created by national supervisors should also reflect the various types of transactions that are most prevalent in the national banking system. For example, non-face-to-face opening of accounts may be more prevalent in one country than another. For this reason the customer identification procedures may differ between countries.

6. Some identification documents are more vulnerable to fraud than others. For those that are most susceptible to fraud, or where there is uncertainty concerning the validity of the document(s) presented, the bank should verify the information provided by the customer through additional inquiries or other sources of information.

7. Customer identification documents should be retained for at least five years after an account is closed. All financial transaction records should be retained for at least five years after the transaction has taken place.

8. These guidelines are divided into two sections covering different aspects of customer identification. Section A describes what types of

information should be collected and verified for natural persons seeking to open accounts or perform transactions. Section B describes what types of information should be collected and verified for institutions and is in two parts, the first relating to corporate vehicles and the second to other types of institutions.

9. All the terms used in these guidelines have the same meaning as in the *Customer due diligence for banks* paper.

A. Natural Persons

10. For natural persons the following information should be obtained, where applicable:

- legal name and any other names used (such as maiden name);
- correct permanent address (the full address should be obtained; a Post Office box number is not sufficient);
- telephone number, fax number, and e-mail address;
- date and place of birth;
- nationality;
- occupation, public position held and/or name of employer;
- an official personal identification number or other unique identifier contained in an unexpired official document (e.g. passport, identification card, residence permit, social security records, driving licence) that bears a photograph of the customer;
- type of account and nature of the banking relationship;
- signature.

11. The bank should verify this information by at least one of the following methods:

- confirming the date of birth from an official document (e.g. birth certificate, passport, identity card, social security records);

- confirming the permanent address (e.g. utility bill, tax assessment, bank statement, a letter from a public authority);
- contacting the customer by telephone, by letter or by e-mail to confirm the information supplied after an account has been opened (e.g. a disconnected phone, returned mail, or incorrect e-mail address should warrant further investigation);
- confirming the validity of the official documentation provided through certification by an authorised person (e.g. embassy official, notary public).

12. The examples quoted above are not the only possibilities. In particular jurisdictions there may be other documents of an equivalent nature which may be produced as satisfactory evidence of customers' identity.

13. Financial institutions should apply equally effective customer identification procedures for non-face-to-face customers as for those available for interview.

14. From the information provided in paragraph 10, financial institutions should be able to make an initial assessment of a customer's risk profile. Particular attention needs to be focused on those customers identified thereby as having a higher risk profile and additional inquiries made or information obtained in respect of those customers to include the following:

- evidence of an individual's permanent address sought through a credit reference agency search, or through independent verification by home visits;
- personal reference (i.e. by an existing customer of the same institution);
- prior bank reference and contact with the bank regarding the customer;

- source of wealth;
- verification of employment, public position held (where appropriate).

15. For one-off or occasional transactions where the amount of the transaction or series of linked transactions does not exceed an established minimum monetary value, it might be sufficient to require and record only name and address.

16. It is important that the customer acceptance policy is not so restrictive that it results in a denial of access by the general public to banking services, especially for people who are financially or socially disadvantaged.

B. Institutions

17. The underlying principles of customer identification for natural persons have equal application to customer identification for all institutions. Where in the following the identification and verification of natural persons is involved, the foregoing guidance in respect of such persons should have equal application.

18. The term institution includes any entity that is not a natural person. In considering the customer identification guidance for the different types of institutions, particular attention should be given to the different levels of risk involved.

I. Corporate Entities

19. For corporate entities (i.e. corporations and partnerships), the following information should be obtained:

- name of institution;

- principal place of institution's business operations;
- mailing address of institution;
- contact telephone and fax numbers;
- some form of official identification number, if available (e.g. tax identification number);
- the original or certified copy of the Certificate of Incorporation and Memorandum and Articles of Association;
- the resolution of the Board of Directors to open an account and identification of those who have authority to operate the account;
- nature and purpose of business and its legitimacy.

20. The bank should verify this information by at least one of the following methods:

- for established corporate entities – reviewing a copy of the latest report and accounts (audited, if available);
- conducting an enquiry by a business information service, or an undertaking from a reputable and known firm of lawyers or accountants confirming the documents submitted;
- undertaking a company search and/or other commercial enquiries to see that the institution has not been, or is not in the process of being, dissolved, struck off, wound up or terminated;
- utilising an independent information verification process, such as by accessing public and private databases;
- obtaining prior bank references;
- visiting the corporate entity, where practical;
- contacting the corporate entity by telephone, mail or e-mail.

21. The bank should also take reasonable steps to verify the identity and reputation of any agent that opens an account on behalf of a corporate customer, if that agent is not an officer of the corporate customer.

Corporations/Partnerships

22. For corporations/partnerships, the principal guidance is to look behind the institution to identify those who have control over the business and the company's/partnership's assets, including those who have ultimate control. For corporations, particular attention should be paid to shareholders, signatories, or others who inject a significant proportion of the capital or financial support or otherwise exercise control. Where the owner is another corporate entity or trust, the objective is to undertake reasonable measures to look behind that company or entity and to verify the identity of the principals. What constitutes control for this purpose will depend on the nature of a company, and may rest in those who are mandated to manage funds, accounts or investments without requiring further authorisation, and who would be in a position to override internal procedures and control mechanisms. For partnerships, each partner should be identified and it is also important to identify immediate family members that have ownership control.

23. Where a company is listed on a recognised stock exchange or is a subsidiary of such a company then the company itself may be considered to be the principal to be identified. However, consideration should be given to whether there is effective control of a listed company by an individual, small group of individuals or another corporate entity or trust. If this is the case then those controllers should also be considered to be principals and identified accordingly.

II. Other Types of Institution

24. For the account categories referred to paragraphs 26 to 34, the following information should be obtained in addition to that required to verify the identity of the principals:

- name of account;

- mailing address;
- contact telephone and fax numbers;
- some form of official identification number, if available (e.g. tax identification number);
- description of the purpose/activities of the account holder (e.g. in a formal constitution);
- copy of documentation confirming the legal existence of the account holder (e.g. register of charities).

25. The bank should verify this information by at least one of the following:

- obtaining an independent undertaking from a reputable and known firm of lawyers or accountants confirming the documents submitted;
- obtaining prior bank references;
- accessing public and private databases or official sources.

Retirement Benefit Programmes

26. Where an occupational pension programme, employee benefit trust or share option plan is an applicant for an account the trustee and any other person who has control over the relationship (e.g. administrator, programme manager, and account signatories) should be considered as principals and the bank should take steps to verify their identities.

Mutuals/Friendly Societies, Cooperatives and Provident Societies

27. Where these entities are an applicant for an account, the principals to be identified should be considered to be those persons exercising control or significant influence over the organisation's assets. This will often include board members plus executives and account signatories.

Charities, Clubs and Associations

28. In the case of accounts to be opened for charities, clubs, and societies, the bank should take reasonable steps to identify and verify at least two signatories along with the institution itself. The principals who should be identified should be considered to be those persons exercising control or significant influence over the organisation's assets. This will often include members of a governing body or committee, the President, any board members, the treasurer, and all signatories.

29. In all cases independent verification should be obtained that the persons involved are true representatives of the institution. Independent confirmation should also be obtained of the purpose of the institution.

Trusts and Foundations

30. When opening an account for a trust, the bank should take reasonable steps to verify the trustee(s), the settlor(s) of the trust (including any persons settling assets into the trust), any protector(s), beneficiary(ies), and signatories. Beneficiaries should be identified when they are defined. In the case of a foundation, steps should be taken to verify the founder, the managers/directors and the beneficiaries.

Professional Intermediaries

31. When a professional intermediary opens a client account on behalf of a single client that client must be identified. Professional intermediaries will often open "pooled" accounts on behalf of a number of entities. Where funds held by the intermediary are not co-mingled but where there are "sub-accounts" which can be attributable to each beneficial owner, all beneficial owners of the account held by the intermediary should be identified. Where the funds are co-mingled, the bank should look through to the beneficial owners; however, there may be circumstances which should be set out in supervisory guidance where the bank may not need to look beyond the intermediary (e.g.

when the intermediary is subject to the same due diligence standards in respect of its client base as the bank).

32. Where such circumstances apply and an account is opened for an open or closed ended investment company, unit trust or limited partnership which is also subject to the same due diligence standards in respect of its client base as the bank, the following should be considered as principals and the bank should take steps to identify:

- the fund itself;
- its directors or any controlling board where it is a company;
- its trustee where it is a unit trust;
- its managing (general) partner where it is a limited partnership;
- account signatories;
- any other person who has control over the relationship (e.g. fund administrator or manager).

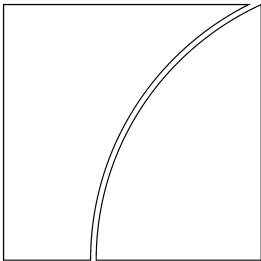
33. Where other investment vehicles are involved, the same steps should be taken as in paragraph 32 where it is appropriate to do so. In addition all reasonable steps should be taken to verify the identity of the beneficial owners of the funds and of those who have control of the funds.

34. Intermediaries should be treated as individual customers of the bank and the standing of the intermediary should be separately verified by obtaining the appropriate information drawn from the itemised lists included in paragraphs 19–20 above.

Basel Committee
on Banking Supervision

448

Bulletin CFB 44/2003



**Sharing of financial
records between
jurisdictions in connection
with the fight against
terrorist financing**

April 2002



BANK FOR INTERNATIONAL SETTLEMENTS

Sharing of financial records between jurisdictions in connection with the fight against terrorist financing

Summary of a meeting of representatives of Supervisors and Legal Experts of G10 Central Banks and Supervisory Authorities on 14 December 2001, Basel, Switzerland

(a) Introduction

1. On 14 December 2001, bank supervisors and legal experts of G10 central banks and supervisory authorities met at the BIS to discuss how to prevent the abuse of the financial system when it is used to finance terrorism, and, specifically, issues relating to the sharing of financial records between jurisdictions to assist in the fight against terrorism. The meeting provided an opportunity for participants to review international developments directed at terrorism, and to consider specific assistance that central banks and banking supervisors might provide. The participants discussed measures that had been taken in their jurisdictions to combat terrorist financing and surveyed mechanisms for the sharing of financial records between national jurisdictions. In many of the countries represented at the meeting, legislation has been or is in the course of being amended to provide for sanctions to deter terrorist activities, including measures to deter terrorist financing.

2. All participants fully embraced the goal of combating terrorism and shared the view of the Chairman of the Basel Committee that measures to impede terrorist financing are critical. The participants agreed with the Chairman that the Basel Committee should add its voice condemning terrorism to that of the United Nations Security Council and the Financial Action Task Force of the OECD.

3. Participants agreed that the size and geographical scope of the international financial system make it imperative to significantly improve coordination and collaboration between all the parties involved if measures to identify and prevent terrorist financing are to succeed. Central banks and bank supervisors are typically not in the front line of these efforts. Nevertheless, because terrorism is a threat to financial stability, the participants agreed that central banks and banking supervisors should lend their expertise and resources to those that are more directly involved, including treasuries, judicial authorities and law enforcement authorities such as financial intelligence units. The collaboration needs to operate both at a domestic level between all parties concerned and also, to the extent possible, at an international level. This means that gateways need to exist for information to be transmitted within and across national borders.

4. Participants reported that even at the domestic level there had been clear evidence of intelligence failures because different strands of information had not been centrally collected and analysed. Many countries have created inter-agency task forces in order to remedy this problem and have become more effective in halting terrorist financing (including improving their responses to the lists of suspected terrorist names being circulated).

5. The focus of the 14 December 2001 meeting was on banking activities and on the possibilities of preventing the global financial system from being misused to support terrorist activities. The participants noted that this cannot be achieved unless financial services providers have effective "know your customer" (KYC) and customer due diligence (CDD) procedures and that some of the methods that might be used by terrorists to move money, such as the postal giro network and private wire transfer systems, may not be within the

jurisdiction of central banks or banking supervisors. This underscores the need to introduce or improve KYC and CDD standards for all categories of institutions that provide financial services.

6. Participants emphasized the need to share information about terrorist financing - including the identities of those who might use the global financial system to support terrorism and the patterns of financing activities associated with such support - between different national jurisdictions. Discussion focused on two mechanisms for information flows (a) from a governmental body in one country to a governmental body in another country, using an official gateway or some less formal channel and (b) within a single financial group (i.e. between a financial entity operating in one country and its head office or parent institution in a different country).

(b) Official gateways for cross-border information sharing

7. The participants identified three official gateways for sharing information between national jurisdictions:

- (i) The classical gateway, usually embodied in a treaty for mutual legal assistance ("MLAT"), provides a legal basis for transmitting evidence that can be used for prosecution and judicial procedures. This is of course not confined to financial crime. This gateway, which typically involves formalised procedures, is not customarily used for supervisory or regulatory matters.
- (ii) The second official gateway involves a communication between financial intelligence units (FIUs) or other bodies set up to fight financial crime. The FIUs, with the task of receiving and analysing suspicious transaction reports on an ongoing basis and maintaining close links with police and customs authorities, are presently mostly engaged in tracking terrorist funds and following up reports of potential terrorist accounts. FIUs share information between themselves informally in the context of investigations, usually on the basis of memoranda of understanding (MOU). The Egmont Group of FIUs has established a model for such MOU. Unlike the MLAT, this gateway is not ordinarily used for obtaining evidence, but it is used for obtaining intelligence that might lead to evidence.
- (iii) The third official gateway is the supervisory channel. In relation to banking activities, the information is normally of a general character, designed to monitor the soundness of the banking group. Increasingly in the recent past, however, enquiries have related more to specific asset or liability accounts because of concerns about reputation and legal risk. A recent example concerns accounts for politically exposed persons. The ability to share information is often defined in the legal framework under which the supervisor operates, but it may also be supported by a MOU. Unlike the MLAT, the MOU is not a treaty and usually is not binding on the governments. Instead, it reflects the mutual understanding of the signing supervisory authorities' policies. The MOU may be especially valuable where other types of entities, such as securities or trading firms, are within the jurisdiction of a specific authority, because that authority could share information on customer transactions throughout a larger segment of the financial market. Information communicated through the supervisory gateway usually is communicated for supervisory purposes only, and may therefore not ordinarily be used as evidence, nor be shared widely among governmental entities.

8. While each of these gateways is used to communicate financial information across a national border, the information received through each respective gateway serves a different purpose. Of course, these purposes may also complement one another with respect to an overall objective like fighting terrorism. If a prosecutor needs information to prosecute a criminal case of terrorism, the prosecutor will ordinarily use a MLAT. If a FIU in a host country learns information suggesting that a branch or subsidiary of a banking group has an account for a known terrorist organisation, the FIU may pass that intelligence information to the FIU in the home country for the group. If a bank supervisor in the jurisdiction where such a branch or subsidiary has the account learns about it, then that host supervisor may well pass the information along to the home supervisor for the Group. The overall fight against terrorism needs coordination among prosecutors, financial intelligence units, and banking supervisors in the affected jurisdictions. While the spirit and level of cooperation demonstrated in the aftermath of September 11th far exceeded past experience, many of the participants in the meeting felt that further work needed to be done to coordinate between interested governmental bodies, within a jurisdiction and, particularly, across national boundaries.

9. The participants felt that this need was demonstrated recently in the case of the circulation of "control lists" of individuals suspected to be involved in terrorism. In particular, both the circulation of the lists within financial groups and the reporting mechanisms for feedback did not operate uniformly. Participants were of the view that the FIU channel is in most cases the most effective gateway in such circumstances. The efficiency of this gateway would, however, be impaired if the involved authorities did not collaborate closely. A breakdown in communication could occur between FIUs, or between an FIU and a banking supervisor within the same country. The participants believed that further work delineating sharing arrangements is desirable, particularly with respect to the fight against terrorism.

(c) Information flow from a financial entity to its head office/parent

10. The first line of defence against terrorist financing is for those involved in terrorism to be denied all support, which includes a denial of access to the financial system. Strenuous efforts have been made over recent years to prohibit the use of the financial system by criminal elements and these efforts are now being reviewed to ensure they reflect the terrorist threat. The identification of the customer is key and this is the object of the Customer Due Diligence paper issued in October 2001 by the Basel Committee on Bank Supervision. That paper emphasises the significant risks, notably reputational risk, for banks that do not have sufficient KYC procedures. The procedures should apply both to the initial identification process and the ongoing monitoring of higher risk accounts. Responsibility for this task lies with the banks' compliance officers under the overall direction of top management and subject to review in the supervisory process.

11. The monitoring of reputational risk needs to be conducted for an institution on a worldwide basis. For that reason, the CDD paper stresses that the risk management process must embrace all foreign branches and subsidiaries, even if they are subject to lower KYC standards in some jurisdictions. Banks require a centralised risk management system that is overseen by the group's chief compliance officer. The centralised risk management system can utilise one of two approaches in obtaining its information:

- (i) The first is the creation of a centralised database or register at the parent bank. However, many foreign branches and subsidiaries are not permitted to transmit the customer files outside of their jurisdiction. In some cases, this may be forbidden by the law of the jurisdiction in which the branch or subsidiary is located. In other cases, particularly where offshore centres offering private banking services are

concerned, the local branch or subsidiary may maintain that its business with nationals of its home country will be handicapped if financial records containing customer names find their way back to the authorities at the headquarters of the parent bank. The reason for this is usually tax-related, but there are other reasons why customers may wish to keep their financial records confidential.

- (ii) In the second approach, a centralised database would not be maintained at the parent bank, but information would be kept at branches and subsidiaries and made available to the parent bank on request, or at the initiative of the branches and subsidiaries when the reputation or liability of the group could be threatened by the relationship. This approach would allow financial groups to determine their own organisational structure, yet branches and subsidiaries would be expected to maintain rigorous risk management systems for due diligence purposes, and the adequacy of these systems would be reviewed by home supervisory authorities. In the case of a relationship with a person believed to be involved in terrorism, the participants felt the relationship should be disclosed to the centralised risk manager. The participants felt that a banking group should require such disclosure as a matter of policy.

12. Participants recognise that the Basel Committee already has taken a number of steps to persuade banks to adopt centralised risk management systems. However, they felt that further attention should be paid to this practice in the light of recent developments, with specific reference to the ability of the group compliance officer to access names of all the bank's customers in its overseas branches and subsidiaries, especially if any of those names were suspected to be associated with terrorism.

(d) Conclusions

13. Participants suggested that the Basel Committee add its voice condemning terrorism to that of the United Nations Security Council and the FATF. The Basel Committee should also acknowledge that terrorism threatens financial stability, and the threat needs to be met with collective actions to identify and halt terrorist financing.

14. The participants believed that adequate means for group wide centralised risk assessment is essential, as the provision of financial services to terrorists would expose the group to material reputational and legal risk. Furthermore, best practices of consolidated home country supervision require that a home country supervisor must know if any foreign branch or subsidiary of a group for which it acted as consolidated supervisor were providing financial services to terrorists. This kind of significant supervisory information needs to reach the consolidated supervisor, in the view of the participants, and must flow across the national border.

15. Participants suggested the Basel Committee consider further work to be done on best practices for controlling reputational and legal risk arising from a relationship with a terrorist organisation by any part of a banking group, such as by remitting the matter to the Cross-border Banking Working Group¹ to provide additional guidance regarding, for example,

¹ In October 2001, the Basel Committee released the Customer Due Diligence for Banks paper that was drafted by the Working Group on Cross-border Banking. This paper explored the risks associated with customer account relationships and established essential elements of know your customer standards, which highlighted

the appropriate roles and responsibilities of individual offices and subsidiaries of a banking organisation and those of its centralised risk management function in detecting and communicating any relationship with a possible terrorist organisation, and to consider the responsibilities and practices to be followed by supervisory authorities to ensure that bank processes in this regard work effectively.

16. Participants suggested further that the Basel Committee consider asking the legal experts of the G10 central banks and supervisory authorities and/or other legal experts (including, if appropriate, FIU experts) to explore current impediments to (i) sharing information on terrorist financing and develop guidelines for passing information across borders to other interested parties, particularly in the case of sharing information between host and home supervisors, and (ii) treating financial groups as single entities for the purpose of sharing information within the group. Other areas for additional work could include developing best practices for the sharing of information by an FIU with a banking supervisor within the same country where the banking supervisor acts as the consolidated supervisor for a banking group where a component of that group has a financial relationship with an identified terrorist, as well as best practices for collecting and sharing information where no FIU exists within a particular country.

the importance of an effective centralised risk management program to effectively control reputational, compliance and legal risks.



**Financial Action Task Force
on Money Laundering**
Groupe d'action financière
sur le blanchiment de capitaux

454

Bulletin CFB 44/2003

**Special Recommendations
on Terrorist Financing**

31 October 2001

FATF Special Recommendations on Terrorist Financing

Recognising the vital importance of taking action to combat the financing of terrorism, the FATF has agreed these Recommendations, which, when combined with the FATF Forty Recommendations on money laundering, set out the basic framework to detect, prevent and suppress the financing of terrorism and terrorist acts.

I. Ratification and implementation of UN instruments

Each country should take immediate steps to ratify and to implement fully the 1999 United Nations International Convention for the Suppression of the Financing of Terrorism.

Countries should also immediately implement the United Nations resolutions relating to the prevention and suppression of the financing of terrorist acts, particularly United Nations Security Council Resolution 1373.

II. Criminalising the financing of terrorism and associated money laundering

Each country should criminalise the financing of terrorism, terrorist acts and terrorist organisations. Countries should ensure that such offences are designated as money laundering predicate offences.

III. Freezing and confiscating terrorist assets

Each country should implement measures to freeze without delay funds or other assets of terrorists, those who finance terrorism and terrorist organisations in accordance with the United Nations resolutions relating to the prevention and suppression of the financing of terrorist acts.

Each country should also adopt and implement measures, including legislative ones, which would enable the competent authorities to seize and confiscate property that is the proceeds of, or used in, or intended or allocated for use in, the financing of terrorism, terrorist acts or terrorist organisations.

IV. Reporting suspicious transactions related to terrorism

If financial institutions, or other businesses or entities subject to anti-money laundering obligations, suspect or have reasonable grounds to suspect that funds are linked or related to, or are to be used for terrorism, terrorist acts or by terrorist organisations, they should be required to report promptly their suspicions to the competent authorities.

V. International co-operation

Each country should afford another country, on the basis of a treaty, arrangement or other mechanism for mutual legal assistance or information exchange, the greatest possible measure of assistance in connection with criminal, civil enforcement, and administrative investigations, inquiries and proceedings relating to the financing of terrorism, terrorist acts and terrorist organisations.

Countries should also take all possible measures to ensure that they do not provide safe havens for individuals charged with the financing of terrorism, terrorist acts or terrorist organisations, and should have procedures in place to extradite, where possible, such individuals.

VI. Alternative remittance

Each country should take measures to ensure that persons or legal entities, including agents, that provide a service for the transmission of money or value, including transmission through an informal money or value transfer system or network, should be licensed or registered and subject to all the FATF Recommendations that apply to banks and non-bank financial institutions. Each country should ensure that persons or legal entities that carry out this service illegally are subject to administrative, civil or criminal sanctions.

VII. Wire transfers

Countries should take measures to require financial institutions, including money remitters, to include accurate and meaningful originator information (name, address and account number) on funds transfers and related messages that are sent, and the information should remain with the transfer or related message through the payment chain.

Countries should take measures to ensure that financial institutions, including money remitters, conduct enhanced scrutiny of and monitor for suspicious activity funds transfers which do not contain complete originator information (name, address and account number).

VIII. Non-profit organisations

Countries should review the adequacy of laws and regulations that relate to entities that can be abused for the financing of terrorism. Non-profit organisations are particularly vulnerable, and countries should ensure that they cannot be misused:

- (i) by terrorist organisations posing as legitimate entities;
- (ii) to exploit legitimate entities as conduits for terrorist financing, including for the purpose of escaping asset freezing measures; and
- (iii) to conceal or obscure the clandestine diversion of funds intended for legitimate purposes to terrorist organisations.