Eidgenössische Finanzmarktaufsicht FINMA
Autorité fédérale de surveillance des marchés financiers FINMA
Autorità federale di vigilanza sui mercati finanziari FINMA
Swiss Financial Market Supervisory Authority FINMA

FINMA-Aufsichtsmitteilung 02/2026

Digitale Betrugsrisiken bei Banken und Personen nach Art. 1*b* BankG

9. April 2026

Laupenstrasse 27, 3003 Bern, Tel. +41 (0)31 327 91 00, www.finma.ch

Inhaltsverzeichnis

1 Einleitung und Begrifflichkeiten

Die FINMA stellt seit Ende 2022 eine kontinuierliche Zunahme von digitalen Betrugsfällen bei Banken (nachfolgend „Institute“) fest. Die neusten technologischen Entwicklungen, insbesondere der Fortschritt im Bereich der künstlichen Intelligenz sowie der digitale Wandel zur Steigerung der Effizienz mittels Automatisierungen – etwa im Bereich des Online-Zugriffs auf Bankkonti oder Zahlungsabwicklungen durch beispielsweise *Instant Payment* – drohen diesen Trend weiter zu verstärken.

Aufgrund der diesen digitalen Betrugsfällen zugrundeliegenden Vielfältigkeit lässt sich keine abschliessende, allgemeingültige Definition von *Digital Fraud* formulieren. Statt einer starren Definition wird der Begriff daher meist funktional verstanden: Digitale Betrugsformen umfassen betrügerische Handlungen, bei denen digitale Technologien, Informationssysteme oder elektronische Kommunikationsmittel zum Zweck einer Vermögensschädigung zur Täuschung eingesetzt werden. Typische Phänomene umfassen beispielsweise Identitätsbetrug sowie -diebstahl, oder wenn Personen aufgrund betrügerischer Absichten Dritter dazu motiviert werden, auf digitalem Weg Bankkonti zu eröffnen, die später in betrügerischer Weise missbraucht werden. Auch die Entwendung von Login-Daten sowie die digitale Kontoeröffnung mit gefälschten Ausweisdokumenten, stellen erhebliche Risiken dar.[1]

Digitale Betrugsrisiken können Banken und Personen nach Art.1*b* des Bankengesetzes vom 8. November 1934 (BankG; SR *952.0*) in mehrfacher Hinsicht vor Herausforderungen stellen: Einerseits können digitale Betrugsrisiken die Banken und ihr Personal direkt betreffen, beispielsweise durch CEO-Betrug[2] und Überweisungsbetrug. Andererseits können auch Bankkundinnen und Bankkunden Opfer von digitalem Betrug sein, etwa durch *Real Time Phishing*.[3] In solchen Konstellationen gilt es die Betrugstrends umgehend durch die Institute zu identifizieren und allfällige Sicherheitslücken zu schliessen, um weitere Missbrauchs- und Manipulationshandlungen zu verhindern. Dies gilt namentlich dann, wenn die digitale Infrastruktur oder die Identität der Institute gezielt und systematisch für betrügerische Zwecke missbraucht wird. Ein strukturelles Versagen kann in solchen Fällen nicht nur erhebliche rechtliche Risiken für das Institut zur Folge haben, sondern auch einen erheblichen Reputationsverlust verursachen, der das Vertrauen der Kundinnen und Kunden nachhaltig beeinträchtigen kann. Bei digitalen Betrugsrisiken handelt es sich somit um wesentliche operationelle Risiken

[1] Hinzu kommen bspw. *Client Impersonation*, verschiedene Arten von *Phishing*, Kontoübernahmen und *Authorised Push Payments* sowie verschiedene Formen von *Social Engineering*, insbesondere *CEO-Fraud* und *Wire Fraud.* Studien zeigen zudem, dass bei aufgedeckten Betrugsversuchen im europäischen Finanz- und Zahlungsverkehrssektor oftmals generative KI eingesetzt wird.

[2] Betrugsmaschen, die auf angeblich dringenden Zahlungsaufforderungen von Kaderpersonen beruhen.

[3] Betrugsmaschen, bei denen Angreifer interaktiv Bankzugangsdaten oder Autorisierungscodes zur Kontoübernahme und Auslösung betrügerischer Zahlungen ergattern.

sowie Rechts- und Reputationsrisiken, denen das Institut jederzeit durch geeignete organisatorische und technische Massnahmen in erhöhtem Masse Rechnung tragen muss.

Die FINMA hat Ende 2025 bei 19 Banken verschiedener Aufsichtskategorien eine Umfrage zum Thema *Digital Banking* durchgeführt. Mit dieser Aufsichtsmitteilung teilt sie Erkenntnisse mit, die sie im Rahmen dieser Umfrage und ihrer weiteren Aufsichtstätigkeiten gewonnen hat. Ziel ist die Sensibilisierung von Banken und Personen nach Art. 1*b* BankG für digitale Betrugsrisiken zwecks Aufbau eines wirksamen Abwehrdispositivs.

2 Rechtliche Grundlagen

Banken und Personen nach Art. 1*b* BankG haben im Rahmen ihrer Geschäftstätigkeiten ein angemessenes Risikomanagement vorzusehen. Das Risikomanagement muss dabei die gesamte Geschäftstätigkeit erfassen und so organisiert sein, dass sich alle wesentlichen Risiken feststellen, bewerten, steuern und überwachen lassen. Zu diesen Risiken zählen auch operationelle Risiken sowie Rechts- und Reputationsrisiken. Für Banken und Personen nach Art. 1*b* BankG ergibt sich diese Pflicht zur Erfassung, Begrenzung und Überwachung ihrer Risiken primär aus den organisatorischen Anforderungen gemäss Art. 1*a*, Art. 1*b*, Art. 3 Abs. 2 Bst. a und Art. 3*c* BankG i.V.m. Art. 12 Abs. 2 und Art. 14*e* der Bankenverordnung vom 30. April 2014 (BankV; SR *952.02*). Die FINMA hat ihre diesbezügliche Aufsichtspraxis im Rundschreiben 2023/1 „Operationelle Risiken und Resilienz – Banken“ konkretisiert. Im Bereich der Geldwäschereiprävention ergeben sich entsprechenden Sorgfaltspflichten insbesondere aus Art. 3–6 des Geldwäschereigesetzes vom 10. Oktober 1997 (GwG; SR *955.0*) sowie Art. 13 ff. der Geldwäschereiverordnung-FINMA vom 3. Juni 2015 (GwV-FINMA; SR *955.033.0*). Die Aufsichtspraxis im Kontext der digitalen Erbringung von Finanzdienstleistungen wurde zudem im FINMA-Rundschreiben 2016/7 „Video- und Online-Identifizierung“ konkretisiert.

3 Erkenntnisse und Hinweise aus der Umfrage *Digital Banking*

Die Umfrage zum Thema *Digital Banking* offenbart bei den befragten Instituten verschiedene Defizite im Umgang mit digitalen Betrugsrisiken. Daraus ergibt sich insbesondere ein konkreter Handlungsbedarf bezüglich dem operationellen Risikomanagement bei digitalen Betrugsrisiken (inkl. Governance und Risikomanagement, der Erkennung und Reaktion auf solche Risiken), sowie im Umgang mit Fällen betrügerischer Verwendung digital eröffneter Konten sowie im Rahmen der Geldwäschereiprävention.

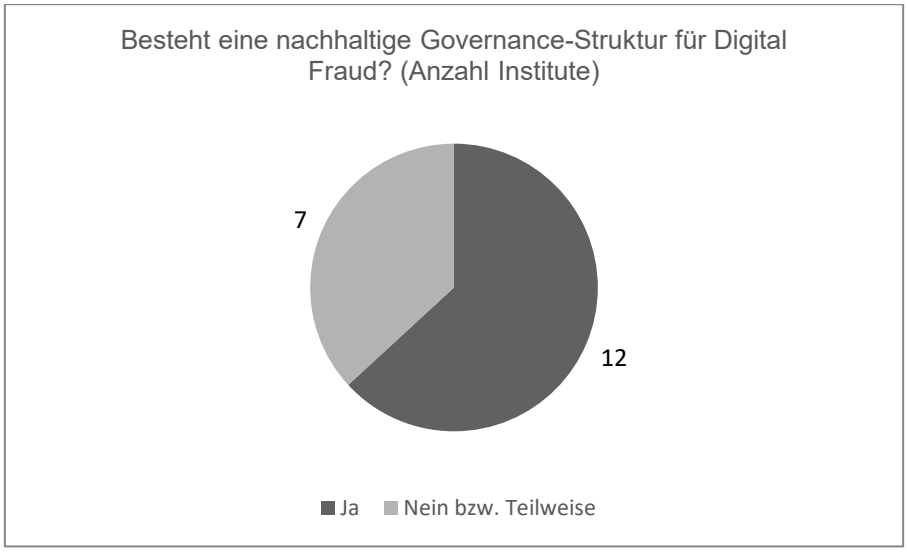
3.1 Operationelles Risikomanagement bei digitalen Betrugsrisiken

3.1.1 Governance und Risikomanagement im Zusammenhang mit digitalen Betrugsrisiken

Erkenntnisse

Die Umfrage zeigte, dass es vielen Instituten an klaren Governance-Strukturen hinsichtlich digitaler Betrugsrisiken fehlt. Dies, obwohl digitale Betrugshandlungen auf dem Schweizer Finanzmarkt sowohl zu erheblichen Verlusten bei Kundinnen und Kunden als auch bei Finanzinstituten führen können. So war Betrug gemäss Jahresbericht des Banken-Ombudsman 2024 die häufigste Problemursache der unterbreiteten Fälle.[4]

Zwölf von 19 Instituten gaben in der Umfrage an, über nachhaltige Governance-Strukturen im Bereich *Digital Fraud* zu verfügen. Es liess sich diesbezüglich feststellen, dass diese zumeist aus Personalunionen[5] bestehen – ohne klare Aufgabenzuweisungen, Verantwortlichkeiten sowie ohne eindeutige und dokumentierte Regelung der Kompetenzen.

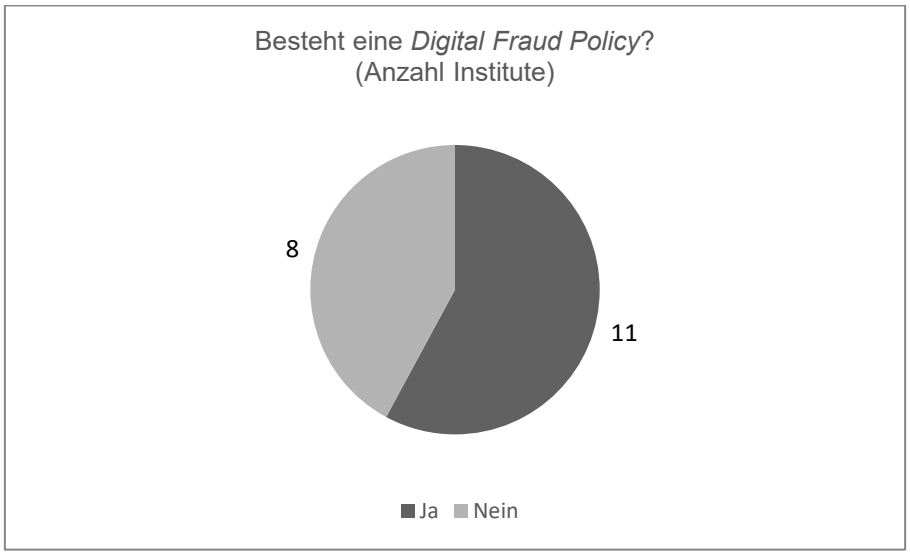


Des Weiteren gaben drei der befragten Institute an, über gar kein Steuerungsgremium für digitale Betrugsrisiken zu verfügen. Positiv zu erwähnen sind hingegen die Resultate durch den Einsatz von interdisziplinären *Fraud Desks* zur umfassenden Steuerung von Anforderungen, Kontrollen und Prozessen im Bereich des digitalen Betrugsrisikomanagements mit klarer Unterstellung.

[4] Vgl. Jahresbericht des Schweizer Banken-Ombudsman 2024, S. 8.

[5] Bspw. aus *Security Operations*, *Payments*, *Risk Management* und IT

Vielen der befragten Institute mangelt es an eigenständigen Weisungen zum Umgang mit digitalen Betrugsrisiken. Diesbezügliche Themenfelder werden stattdessen mittels anderweitiger Weisungen adressiert (namentlich betreffend Mitarbeitergeschäfte, Geldwäscherei oder Informationssicherheitsweisungen), ohne, dass diese Weisungen aufeinander abgestimmt sind. Entsprechend verfügen acht der 19 Institute (42 Prozent) über keine sog. *Digital Fraud Policy*.



Zudem weist nur ca. die Hälfte der befragten Institute in ihrer Berichterstattung an die Geschäftsleitung regelmässig Kennzahlen im Zusammenhang mit *Digital-Fraud*-Fällen aus.

Hinweise

Die FINMA macht darauf aufmerksam, dass digitale Betrugsrisiken wesentliche Risiken für das Institut darstellen können, die durch die Regelung von internen Zuständigkeiten und Verfahren umfassend festgestellt, bewertet, gesteuert und überwacht werden müssen. Gemäss Aufsichtspraxis der FINMA haben Institute im Rahmen ihrer Governance und ihrem Risikomanagement die zur Minderung dieser operationellen Risiken notwendigen Strukturen, Vorgaben, Prozesse und Kontrollen einzurichten.

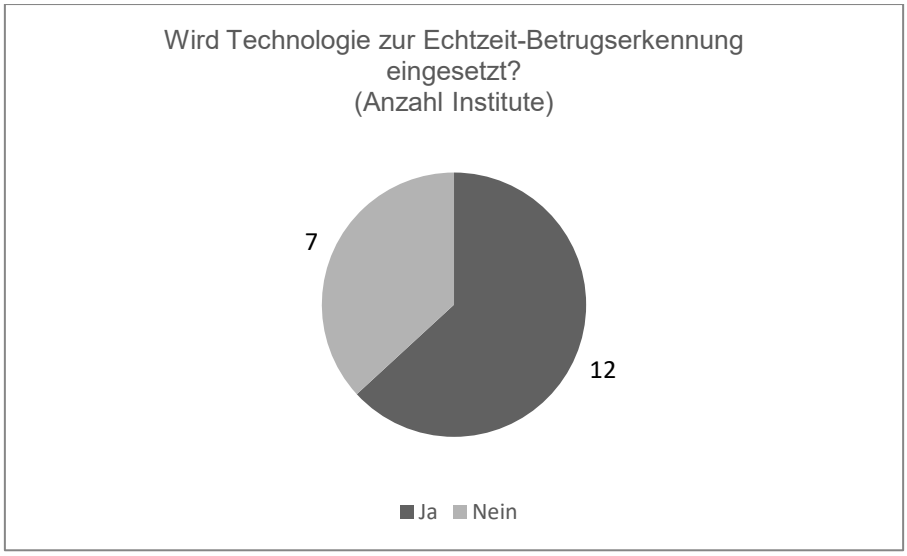
3.1.2 Erkennung und Reaktion hinsichtlich digitaler Betrugstrends

Erkenntnisse

Die Umfrage ergab, dass 26 Prozent der befragten Institute über keinerlei Prozesse zur Erkennung und Antizipation von digitalen Betrugstrends (sog. *Horizon Scanning*) verfügen. Das bedeutet, dass diese Institute relevante Betrugsbedrohungen und -szenarien für ihre digitalen Dienstleistungen nicht

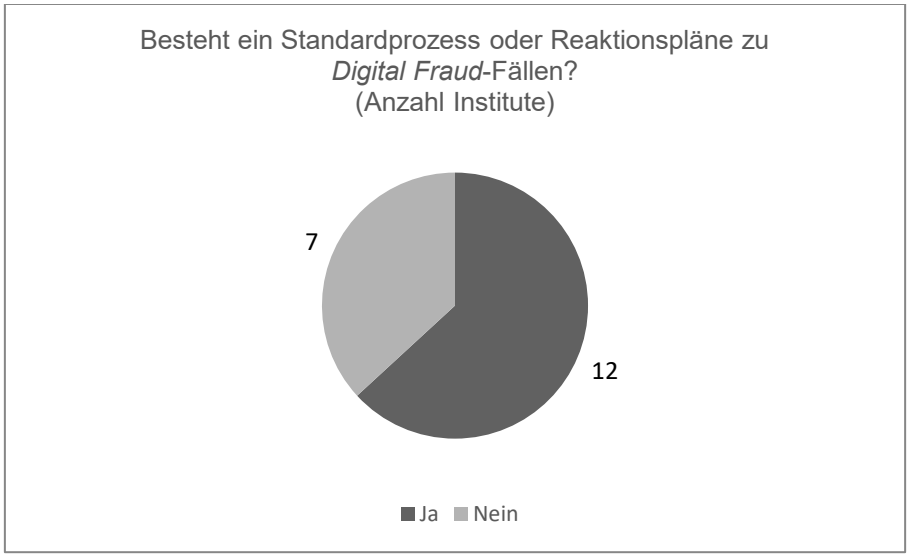
proaktiv identifizieren und dementsprechend auch keine Vorkehrungen treffen können.

Des Weiteren setzen zwölf von 19 Instituten Technologien zur Echtzeit-Betrugserkennung ein.



Umgekehrt gaben sieben Institute an, Indikatoren laufender digitaler Betrugskampagnen gar nicht oder nur manuell bzw. fallbasiert auszuwerten. Dies erschwert die übergreifende Erkennung relevanter Muster auf mehreren Ebenen. Aufgrund der starken Abhängigkeit von Dienstleistern können des Weiteren nicht alle Institute relevante Erkennungsregeln zeitnah anpassen, was eine prompte Reaktion auf erkannte Betrugsserien oder Betrugsmuster gefährdet.

Die Umfrage hat zudem ergeben, dass auch die Standardisierung der Reaktionsprozesse und die entsprechenden Vorgaben verbesserungswürdig sind: Bei sieben der 19 befragten Institute fehlt es an einem Standardprozess oder an Reaktionsplänen zu *Digital Fraud*-Fällen.



Des Weiteren gaben lediglich sieben von 19 Instituten an, ihre Reaktionspläne mindestens einmal pro Jahr zu aktualisieren. Die übrigen befragten Institute nehmen eine Aktualisierung ihrer Reaktionspläne ausschliesslich anlassbezogen, das heisst erst nach dem Ereignisfall ad hoc, vor. Generell werden Reaktionsfristen im Zusammenhang mit Meldungen zu digitalen Betrugsfällen von den meisten Instituten weder vorgeschrieben, noch gemessen oder überprüft. Nur wenige der befragten Institute bieten eine 24/7 Verfügbarkeit ihrer Meldekanäle an. Die wenigsten Institute verfügen ausserdem über spezifische Kanäle für Betrugsmeldungen. Stattdessen nehmen sie solche Meldungen über die allgemeine Telefon-Hotline entgegen.

Hinweise

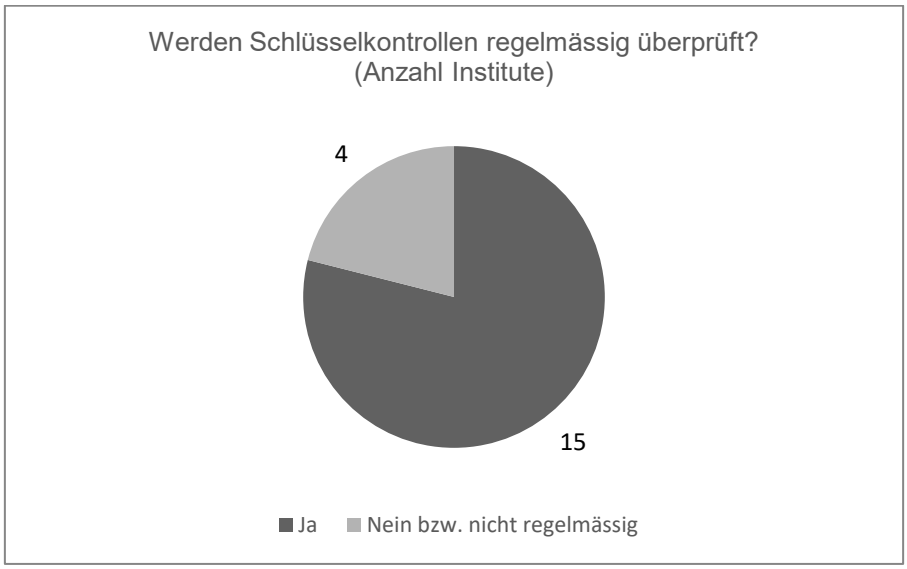
Die wirksame Bekämpfung von digitalen Betrugsrisiken erfordert eine proaktive, sowie zeitnahe, systematische und institutsweite Erkennung und die umgehende Einleitung von angemessenen Gegenmassnahmen im Eintrittsfall. Unzureichende Erkennungs- und verlangsamte Reaktionsmechanismen können dazu führen, dass sich Betrugsfälle häufen oder an Schwere zunehmen, Vermögenswerte unwiederbringlich abfliessen und geldwäschereirelevante Transaktionen nicht rechtzeitig unterbunden werden.

3.1.3 Kontrollen und Wirksamkeitsüberprüfung der Betrugsprävention

Erkenntnisse

Drei der befragten Institute setzen gar keine technischen Kontrollen wie *Geo-blocking*, *IP-Risk Rating* oder *Device Fingerprinting* zur Authentifizierung von Kundinnen und Kunden ein.

Schlüsselkontrollen als zentrales Kontrollinstrument zu digitalen Betrugsrisiken fehlen bei rund 20 Prozent der befragten Institute oder werden nicht regelmässig bezüglich ihrer Wirksamkeit überprüft.



Einzelne befragte Institute gaben an, ihre Mitarbeitenden nicht weiter zu Risiken im Bereich *Digital Fraud* zu schulen. Die übrigen Institute führen zwar Schulungen durch, jedoch wird in diesen Schulungen oftmals nur generisch über digitale Betrugsrisiken informiert und nicht rollenbasiert unter Berücksichtigung des Tätigkeitsbereichs und der Risikolage der teilnehmenden Mitarbeitenden (z.B. Kundenberaterinnen und -berater). Die verwendeten Mittel und der Schulungsrhythmus zur Sensibilisierung der Mitarbeitenden und Kundinnen und Kunden variieren zudem sehr stark. Auch identifizieren nicht alle befragten Institute besonders verwundbare oder exponierte Kundensegmente für digitale Betrugsrisiken.

Hinweise

Da Massnahmen zur digitalen Betrugsprävention und -bekämpfung typischerweise auf verschiedenen Ebenen greifen, sind deren Integration und Wirksamkeit umfassend zu rapportieren und regelmässig durch angemessene Kontrollen zu überprüfen.

Digitale Betrugsrisiken sind dynamisch und entwickeln sich fortlaufend weiter. Die regelmässige Schulung der Mitarbeitenden sowie die Sensibilisierung der Kundinnen und Kunden stellen daher wichtige Präventionsinstrumente dar, um das Bewusstsein für mögliche Betrugsmuster zu schärfen.

3.2 Betrügerische Verwendung digital eröffneter Konten

Erkenntnisse

Im Rahmen ihrer Aufsichtstätigkeit stellt die FINMA fest, dass sich über die letzten Jahre Betrugsfälle häufen, die über digital eröffnete Kundenkonten abgewickelt werden. Kriminelle Organisationen versuchen durch den Einsatz zunehmend sophistizierter technischer Mittel unrechtmässig Bankkonten zu eröffnen, über die inkriminierte Gelder abgewickelt werden können. So entwickeln und nutzen sie fortlaufend komplexere technische Methoden, um regulatorische Kontrollmechanismen bei der Kontoeröffnung zu unterlaufen.

Im Zusammenhang mit der digitalen Eröffnung von Kundenbeziehungen stellt insbesondere die betrügerische Kontoeröffnung (gefälschte Ausweise oder Identitätsmissbrauch) eine Gefahr dar. Diese Risikolage erhöht sich durch den verstärkten Einsatz von künstlicher Intelligenz, Videomanipulationssoftware und *Deepfake*-Technologien. Kriminelle Organisationen nutzen die neuen Möglichkeiten der Technik umfassend und manipulierte Videos oder gefälschte Ausweisdokumente sind zunehmend schwerer zu erkennen. Die Daten der Umfrage zeigen jedoch keine klare Bestätigung, dass bei der digitalen Eröffnung von Bankbeziehungen vermehrt betrügerisch vorgegangen wird. Auffällig ist jedoch die Häufung der MROS-Meldungen im Zusammenhang mit Kundenbeziehungen, die digital eröffnet wurden. Es häufen sich nebst betrügerischer Kontoeröffnungen insbesondere Fälle, bei denen Personen mit betrügerischen Mitteln und unter Vorspielen falscher Tatsachen dazu gebracht werden, digital Konten zu eröffnen und die Autorisierung über die Konten nach Eröffnung an kriminelle Dritte zu übergeben. Weiter erlangen kriminelle Personen mit Mitteln der Cyberkriminalität (bspw. über *Phishing*-Attacken) Verfügungsgewalt über fremde Konten. Die Problematik dabei ist, dass die Kontoeröffnung oftmals mit gültigen Ausweisdokumenten vorgenommen wird, der Eröffnungsprozess somit nach den geltenden Sorgfaltspflichten erfolgt. Der eigentliche betrügerische Akt erfolgt sodann in einem weiteren Schritt, indem Dritte die Verfügungsgewalt über die Konten erlangen.

Hinweise

Flankierenden Sicherheitsmechanismen kommen aufgrund der erhöhten Risikolage im Rahmen der digitalen Kontoeröffnung eine zentrale Bedeutung zu. Diese betreffen beispielsweise die Nutzung von technischen Möglichkeiten zur Erkennung von *Deepfakes* und manipulierten Videos. Zudem sind die Mitarbeitenden im Rahmen eines angemessenen Risikomanagements regelmässig in Bezug auf diese Entwicklungen aus- und weiterzubilden (vgl. auch Rz 8 FINMA-RS 16/7). Die generellen Risiken einer digitalen Eröffnung von Kundenbeziehungen und die Risiken von unautorisierten Kontozugriffen sollten zudem nicht isoliert betrachtet werden, sondern in Rahmen einer umfassenden digitalen Betrugspräventionsstrategie mitberücksichtigt werden.

3.3 Geldwäschereiprävention

Erkenntnisse

Die Umfrage zeigt, dass die relative Anzahl an Geldwäscherei-Verdachtsmeldungen im Zusammenhang mit (Internet-)Betrugsfällen, falscher Identität, Identitätsdiebstahl, unberechtigtem Zugriff auf Konten, *Money Muling* o.ä. unter den befragten Instituten bis um den Faktor 10 variiert. Der Anteil der bankintern generierten Hinweise, welche zu MROS-Verdachtsmeldungen führen, schwankt zudem zwischen 12 und 78 Prozent. Insgesamt deuten die Antworten aus der Umfrage damit auf deutliche Unterschiede in der Effektivität der Geldwäscherei-Dispositive, -Systeme und -Prozesse bezüglich der Entdeckung von Betrugsszenarien zwischen den Instituten hin.

Die erhobenen *Know-Your-Customer*-Informationen (KYC) sind gemäss der Umfrage durchgehend relativ knapp. Die meisten Institute verzichten zudem darauf, die erhobenen KYC-Informationen für das Transaktionsmonitoring überhaupt zu verwenden, z.B. mittels unterschiedlicher Szenarien oder Limiten. Die KYC-Informationen werden in der Regel erst bei konkreten Abklärungen zur Plausibilisierung hinzugezogen. Im Transaktionsmonitoring sind die Betragshöhen, ab welchen bei Privatkundinnen und -kunden mit tiefem bzw. normalem Risiko Durchlauftransaktionen als Transaktionen mit erhöhten Risiken (TmeR) erkannt werden, bei den meisten befragten Instituten relativ hoch angesetzt (CHF 100 000 oder 200 000). Dies deutet auf wenig sophistizierte Systeme hin, welche TmeR hauptsächlich mit starren Limiten anstatt mit spezifischen Szenarien identifizieren. Entsprechend schwierig dürfte es für diese Institute sein, digitale Betrugsfälle im Rahmen des Transaktionsmonitorings zu identifizieren.

Hinweise

Die FINMA ruft den Instituten in Erinnerung, dass die Geldwäscherei-Dispositive, sowie die verwendeten Systeme und Prozesse der Institute ausreichend effektiv sein müssen, um digitale Betrugsfälle und *Money Muling*-Fälle raschmöglichst aufdecken zu können. Insbesondere müssen die Transaktionsüberwachungssysteme in der Lage sein, potenzielle Verdachtsfälle umgehend zu identifizieren.

4 Fazit

Banken und Personen nach Art. 1*b* BankG haben eine angemessene Governance und ein effektives Risikomanagement zur Erkennung, Begrenzung und Kontrolle von digitalen Betrugsrisiken vorzusehen, das sich über die gesamte Geschäftstätigkeit erstreckt und so organisiert ist, dass sich alle wesentlichen Risiken feststellen, bewerten, steuern und überwachen lassen.

Dazu gehören auch digitale Betrugsrisiken bei der digitalen Eröffnung von Kundenbeziehungen in Zusammenhang mit unautorisierten Kontozugriffen. Um damit verbundene erhebliche Rechts- und Reputationsrisiken angemessen überwachen und präventiv tätig werden zu können, bedürfen Institute klare Führungsinstrumente und -strukturen, Prozesse und Verantwortlichkeiten, wirksame Detektions- und Reaktionsfähigkeiten, ein ausgereiftes Transaktionsüberwachungssystem im Bereich Geldwäscherei sowie zielgerichtete Instrumente zur Überprüfung der Wirksamkeit von Kontrollen. Bei gehäuft auftretenden Betrugsfällen ist die Wirksamkeit des Dispositivs zur Identifikation und Abwehr solcher Vorfälle zeitnah zu überprüfen und bei Bedarf durch zusätzliche Massnahmen zu ergänzen. Dies kann auch temporäre Einschränkungen hinsichtlich der Erbringung einzelner Dienstleistungen umfassen, die zu solchen digitalen Betrugsfällen führen.