3 Défaillances de sécurité importantes dans le domaine informatique

DÉCISION de l'Autorité fédérale de surveillance des marchés financiers FINMA du (…)

Organisation administrative appropriée (art. 3 al. 2 let. a LB; art. 9 al. 2 OB); secret bancaire (art. 47 LB).

1. Une banque doit disposer d'une organisation appropriée lui permettant de garantir la confidentialité des données des clients (Cm 73-75).
2. Même en cas de perte de données clients due à des agissements criminels, la banque doit prendre toutes les précautions organisationnelles requises permettant d'éviter une telle perte (Cm 76-97).

Angemessene Verwaltungsorganisation (Art. 3 Abs. 2 Bst. a BankG; Art. 9 Abs. 2 BankV); Bankkundengeheimnis (Art. 47 BankG).

1. Eine Bank muss über eine angemessene Organisation verfügen, welche die Vertraulichkeit von Kundendaten jederzeit garantiert (Rz. 73–75).

2. Auch wenn der Verlust von Bankkundendaten auf einen kriminellen Hintergrund zurückzuführen ist, hat die Bank alle erforderlichen organisatorischen Vorkehren zu treffen, welche einen solchen Verlust verhindern (Rz. 76–97).

Organizzazione adeguata (art. 3 cpv. 2 lett. a LBCR; art. 9 cpv. 2 OBCR); segreto bancario (art. 47 LBCR).

1. Una banca deve disporre di un'organizzazione adeguata che garantisca in ogni momento la riservatezza dei dati dei clienti (nm. 73-75).
2. Anche se la fuga di dati dei clienti è riconducibile a un disegno criminoso, la banca deve adottare tutte le misure organizzative necessarie tese a impedire una tale perdita (nm. 76-97).

Résumé des faits

Suite à un vol de données survenu auprès de la banque X._____, la FINMA a ouvert une procédure à son encontre. Au cours de l'instruction, la FINMA a examiné l'organisation de la banque et de son département IT, les circonstances du vol de données et son étendue, les problèmes de sécurité du système IT et leur évolution ainsi que les mesures prévues pour améliorer la sécurité IT. Elle s'est fondée sur les renseignements de la banque et les investigations d'un consultant externe mandaté par cette dernière. Il est ressorti que le vol portait sur une quantité importante de données personnelles et financières de clients. L'auteur présumé du vol a pour l'essentiel profité de ses accès et de ses connaissances en qualité d'employé du département IT de la banque ainsi que des faiblesses des contrôles, en particulier au niveau de la gestion des accès et du développement de programmes informatiques. Sur la base d'anciens rapports de l'audit interne et du consultant externe, la FINMA a constaté que l'organisation et la sécurité du système informatique IT de la banque souffrait, au moment où le vol a vraisemblablement eu lieu, d'un grand nombre de faiblesses, dont plusieurs à hauts risques. La banque avait alors pris des mesures correctrices qui étaient toutefois insuffisantes pour remédier à certaines faiblesses de nature structurelle. Depuis lors, la banque a entrepris d'importantes mesures supplémentaires.

Extrait des considérants

A. Compétence de la FINMA et législation applicable

(…)

1. La pleine garantie du secret bancaire constitue une condition d'autorisation et de garantie d'une activité irréprochable

(73) Le devoir de confidentialité particulier du banquier ou « secret bancaire » est fondé sur les droits de la personnalité de ses clients, qui protègent la vie privée au niveau économique (art. 27 du Code civil ; RS 210), sur le droit du mandat (art. 398 al. 2 du Code des obligations ; RS 220), sur la disposition pénale de l'art. 47 LB ainsi que sur la loi sur la protection des données (Carlo Lombardini, Droit bancaire suisse, 2e éd., Zurich/Bâle/Genève 2008, p. 965-966 ; Beat Kleiner/Renate Schwob/Christoph Winzeler, in : Bodmer/Kleiner/Lutz, Kommentar zum Schweizerischen Bankengesetz, Zurich 2009, ad. art. 47, n° 1-7).

(74) La pleine garantie du respect du secret bancaire de sa clientèle constitue une des conditions d'autorisation et d'organisation qu'une banque doit respecter en tout temps (Bulletin CFB n° 21, p. 24, consid. 3 a). Une banque doit prendre les mesures organisationnelles internes nécessaires pour faire en sorte que le secret bancaire ne puisse pas être violé (Lombardini, op. cit., p. 969, n° 6 et 7). Sont soumis au secret bancaire et protégés par l'art. 47 LB tous les secrets confiés à une personne en qualité d'organe, d'employé, de mandataire ou de liquidateur d'une banque ou les éléments dont cette personne a eu connaissance en raison de sa charge ou de son emploi. Sont ainsi couvertes par le secret bancaire l'existence même du rapport contractuel avec une banque, les connaissances issues d'une relation d'affaires entre la banque et le client, notamment les contrats bancaires mais également toutes les requêtes et

offres de relations bancaires ainsi que toutes les transactions et les opérations que la banque fait avec ses clients, qu'elles soient ou non de nature bancaire (Lombardini, op. cit., p. 967 ; Kleiner/Schwob/Winzeler, op. cit., ad. art. 47, n° 8). La FINMA n'assume en principe pas de fonction de surveillance relative au secret bancaire. Toutefois, si des violations graves du secret bancaire indiquant l'existence de lacunes organisationnelles de la banque survenaient, la FINMA pourrait ordonner une enquête et prendre les mesures nécessaires sous l'angle de la garantie du respect d'une activité irréprochable (art. 3 al. 2 let. c LB) (Kleiner/Schwob/Winzeler, op. cit. ad. art. 47, n° 386).

(75) Ainsi, du point de vue du droit de la surveillance, une banque doit en tout temps disposer d'une organisation lui permettant de garantir que la confidentialité des données qui sont soumises au secret bancaire ne puisse pas être violée, même en présence d'éventuels éléments criminels internes. Dans la mesure où elle gère ces données de manière informatisée, ces exigences d'organisation s'appliquent également à l'organisation de son système informatique. A défaut, la banque ne remplit pas ses conditions d'autorisation et ne fournit pas la garantie d'une activité irréprochable.

2. Exigence d'une organisation irréprochable du secteur informatique en tant que condition d'autorisation et de garantie d'une activité irréprochable

(76) Une banque, ou un négociant, doit disposer d'une organisation adéquate correspondant à son activité (art. 3 al. 2 let. a LB ; art. 7 et ss de l'ordonnance sur les banques [OB] ; RS 952.02 ; art. 10 al. 2 let. a LBVM ; art. 19 et ss de l'ordonnance sur les bourses [OBVM] ; RS 954.11). L'organisation irréprochable du secteur informatique d'une banque fait partie des conditions d'autorisation de l'art. 3 LB qui doivent être respectées en tout temps (Bulletin CFB n° 21 (1991), p. 24, consid. 2 a ; Rapport de gestion CFB 2004, p. 53). Elle est indispensable à une banque pour lui permettre

une surveillance appropriée de sa gestion (art. 3 al. 2 let. a LB) ainsi que pour offrir la garantie du respect d'une activité irréprochable (art. 3 al. 2 let. c LB). La banque doit fixer dans un règlement ou dans des directives internes les principes lui permettant de déterminer, limiter et contrôler les risques liés à son activité, notamment les risques opérationnels, juridiques et de réputation (art. 9 al. 2 OB). Les buts visés par cette norme sont de plusieurs ordres : il s'agit notamment de protéger les créanciers, de se prémunir contre les risques systémiques ainsi que d'éviter la survenance d'événements propres à mettre en danger la réputation de l'établissement financier concerné et celle de la place financière suisse (Bulletin FINMA 1/2010, p. 51).

(77) Le fonctionnement et la sécurité du système informatique constituent typiquement un risque opérationnel. Comme cela a été ensuite expressément précisé dans les circulaires de l'autorité de surveillance, la structure d'organisation du système informatique doit être clairement mise en place et documentée et ses processus de travail doivent être contrôlés, en particulier en ce qui concerne les accès aux systèmes informatiques et aux données de base (Circ.-FINMA 08/24 « Surveillance et contrôle interne – banques » du 20 novembre 2008, Cm 81-82 et 95 ; anciennement Circ.-CFB 06/6 du 27 septembre 2006). Ce risque peut par ailleurs avoir également des implications importantes au niveau de la situation juridique et de la réputation de la banque.

(78) La doctrine considère également que le système informatique d'une banque doit être performant et sûr. Il représente un élément essentiel de l'organisation administrative de la banque. Un membre de la direction doit en être responsable. Le système doit être revu régulièrement et ses dysfonctionnements analysés et le cas échéant corrigés. Le rapport d'audit doit se prononcer sur l'organisation informatique. Si des tiers interviennent pour la mise en place et l'entretien du système informatique, la banque doit s'assurer de leurs compétences et conserver seule la maîtrise

du système et de ses accès (Lombardini, op. cit., p. 64, n° 79-80). Ainsi, afin de gérer correctement les risques liés à son activité au niveau de son secteur informatique, une banque doit en particulier définir les besoins et les risques liés à la confidentialité des données traitées et mettre en place une organisation et des contrôles permettant effectivement de garantir cette confidentialité, ceci de manière clairement documentée. A défaut, la banque ne remplit pas ses conditions d'autorisation et ne fournit pas la garantie d'une activité irréprochable.

B. Appréciation

1. Manquement à l'obligation de pleine garantie du secret bancaire en tant que condition d'autorisation et de garantie d'une activité irréprochable

(79) La banque a subi un très important vol de données (…). Ces données comprenaient notamment les noms des titulaires de (…) comptes, leurs adresses, dates de naissances, nationalités et numéros de comptes ainsi qu'au moins (…) données d'identification de personnes liées à ces comptes. Le voleur présumé a également soustrait au moins (…) comptes rendus de communications avec des clients. Ces données sont sans aucun doute soumises au secret bancaire. En effet, elles sont de nature à permettre à un tiers de connaître l'existence d'une relation entre la banque et un client particulier.

(80) A cela s'ajoute que le voleur présumé a également soustrait au moins (…) données de positions financières de clients et est parvenu à établir le lien entre les données d'identification des clients et ces données patrimoniales. Ces données, une fois couplées aux données d'identification des clients, sont également soumises au secret bancaire puisqu'elles permettent à un tiers de connaître la situation patrimoniale du client au sein de la banque et même dans certains cas d'établir un profil client.

(81) Ces données ont été rendues accessibles à des tiers (…).

(82) Certes, comme la banque l'a souligné dans le cadre de la présente procédure, ces atteintes sont selon toute vraisemblance le résultat d'une activité illégale d'un employé de la banque et, même en présence d'une organisation adéquate, on ne saurait totalement exclure qu'un employé indélicat emporte et révèle quelques données confidentielles. Néanmoins, il appartient à la banque de prendre des mesures organisationnelles permettant de garantir globalement le secret bancaire, même en présence d'éléments criminels internes. Dans l'éventualité d'un employé ayant la volonté de soustraire des données, ces mesures doivent non seulement en limiter les occasions, mais également garantir que l'étendue d'une éventuelle soustraction sera limitée au niveau de la quantité et de la qualité des données concernées. Ceci d'autant plus que généralement seul un vol de données d'une étendue significative est susceptible de présenter un intérêt pour son auteur.

(83) En l'espèce, compte tenu de la quantité très importante de données volées soumises au secret bancaire et de leur qualité, force est de constater que les mesures d'organisation de la banque n'étaient pas de nature à garantir pleinement le secret bancaire. De ce fait et compte tenu des conséquences négatives des données soustraites pour les clients, pour la banque et pour la réputation de la place financière suisse, ces atteintes au secret bancaire doivent être qualifiées de particulièrement graves. Dès lors, l'organisation de la banque ne satisfaisait pas aux conditions d'autorisation auxquelles elle était soumise et constitue une violation grave de la garantie d'une activité irréprochable au sens de l'art. 3 al. 2 let. c LB.

2. Violation de l'exigence d'organisation irréprochable du secteur informatique en tant que condition d'autorisation et de garantie d'une activité irréprochable

(84) Il ressort des différents rapports de l'audit interne et du consultant externe qu'en (…) l'organisation et la sécurité du système informa-

tique IT de la banque souffrait d'un grand nombre de faiblesses significatives. Celles-ci avaient été résumées par le consultant externe en quatre problématiques clés (...) :

- une interprétation non uniforme de la réglementation suisse ;
- une dissémination inappropriée des données personnelles confidentielles de clients ;
- des mesures de protection des données insuffisantes ;
- un contrôle des activités IT et des activités déléguées inadéquat.

(85) La banque a soutenu dans le cadre de la présente procédure que certaines recommandations du consultant externe allaient au-delà de ce qui était strictement nécessaire au regard de la loi et que les faiblesses y relatives ne pouvaient lui être reprochées. Cet argument est infondé. La loi ne détermine en effet pas elle-même les mesures de sécurité nécessaires mais impose aux établissements bancaires de définir et de mettre en place les mesures d'organisation adaptées à la couverture des risques de leur activité spécifique.

(86) Quoi qu'il en soit, (…), la considération de l'ensemble de ces faiblesses permet de constater que l'organisation informatique de la banque ne correspondait pas à une organisation informatique irréprochable selon les exigences légales et les règles de l'art (…). En effet, une organisation irréprochable du secteur informatique exigeait, au vu de l'activité de la banque, une définition uniforme et clairement documentée : des données confidentielles, de l'organisation des supports informatiques sur lesquels elles étaient conservées, des personnes qui en étaient responsables, des mesures de protection qui leur étaient applicables ainsi que des contrôles des processus de travail en matière IT.

(87) En l'espèce, le rapport du consultant externe a mis en évidence que la banque ne disposait pas en (…) d'une telle organisation. D'abord, la banque n'avait pas correctement défini quelles étaient les données sou-

mises au secret bancaire ou non. Ceci avait pour conséquence que certaines de ces données, considérées à tort comme non sensibles, notamment (…), avaient été disséminées dans divers systèmes informatiques peu sécurisés. L'architecture complexe de ces systèmes informatiques, leurs mesures de protection ainsi que les personnes responsables étaient également insuffisamment définies et documentées. Finalement, les contrôles des activités IT et des activités IT déléguées n'étaient pas clairement documentés ou étaient inadéquats.

(…)

(97) Au vu de ce qui précède, la FINMA a constaté que la banque ne disposait pas d'une organisation informatique irréprochable lui permettant de contrôler d'une manière adéquate les risques liés à son activité durant les années (…) à (…). Son organisation ne satisfaisait ainsi pas entièrement aux conditions d'autorisation exigées par les art. 3 de la LB et 9 al. 2 de l'OB et constituait une violation grave du droit de la surveillance. Il conviendra de s'assurer de la mise en place des mesures correctrices importantes annoncées par la banque dans les délais prévus par celle-ci.

(…)

Dispositif