3 Services informatiques à l'étranger et secret professionnel du banquier

DÉCISION de l'Autorité fédérale de surveillance des marchés financiers FINMA du 8 décembre 2010

Secret professionnel du banquier (art. 47 LB et art. 43 LBVM); organisation adéquate pour les succursales (art. 2 al. 1 let. a LB; art. 41 al. 1 let. a OBVM; art. 4 al. 1 let. a OBE-FINMA); externalisation de services informatiques auprès du siège de la maison mère à l'étranger.

1. Les dispositions régissant le secret bancaire ou professionnel doivent aussi être respectées dans les relations entre la succursale suisse d'une banque et son siège à l'étranger (Cm 29-31).
2. Sur le plan organisationnel, une banque doit faire en sorte que la maintenance informatique continue de s'effectuer conformément à la loi également après un changement de titulaire du poste de responsable de la sécurité (Cm 33-39).

Bankkunden- resp. Berufsgeheimnis (Art. 47 BankG und Art. 43 BEHG); angemessene Verwaltungsorganisation einer Zweigniederlassung (Art. 2 Abs. 1 Bst. a BankG; Art. 41 Abs. 1 Bst. a BEHV; Art. 4 Abs. 1 Bst. a ABV-FINMA); Outsourcing von Informatikdienstleistungen an das ausländische Mutterhaus.

1. Das Bankkunden- resp. Berufsgeheimnis ist grundsätzlich auch im Verhältnis zwischen einer Schweizer Zweigniederlassung einer Bank und dem Hauptsitz im Ausland zu beachten (Rz. 29–31).
2. Eine Bank hat organisatorisch dafür zu sorgen, dass der sicherheitstechnische Unterhalt ihrer IT-Systeme auch nach dem Wechsel des Sicherheitsverantwortlichen weiterhin gesetzeskonform funktioniert (Rz. 33–39).

Segreto bancario risp. professionale (art. 47 LBCR e art. 43 LBVM); organizzazione adeguata di una succursale (art. 2 cpv. 1 lett. a LBCR; art. 41 cpv. 1 lett. a OBVM; art. 4 cpv. 1 lett. a OBE-FINMA); outsourcing di servizi informatici presso la casa madre estera.

1. In linea di principio, il segreto bancario risp. professionale deve essere osservato anche nel rapporto tra la succursale svizzera di una banca e la sede principale all'estero (nm. 29-31).
2. Una banca deve provvedere dal punto di vista organizzativo a che la manutenzione a livello della sicurezza tecnica dei propri sistemi informatici continui a funzionare in maniera conforme alla legge anche in seguito a un cambio nell'organico dei responsabili della sicurezza (nm. 33-39).

Résumé des faits

Une convention (service level agreement ou SLA) passée entre X._____ SA (ci-après la succursale) et le Groupe X._____ règle les services informatiques fournis par la maison mère à sa succursale suisse. Les données relatives à la clientèle soumises au secret bancaire sont conservées dans une base de données séparée de l'application bancaire et localisées sur un serveur en Suisse. Par ailleurs, des restrictions d'accès empêchent le Groupe X._____ de consulter les données clients qui se trouvent en Suisse.

Après le départ du responsable sécurité de la succursale, des collaborateurs du Groupe X._____ ont repris les droits d'administration en la matière, les exerçant depuis l'étranger. A ce moment, aucun collaborateur de X._____ SA ne disposait de l'expertise technique pour assurer cette prestation en Suisse. Ni la direction de X._____ SA ni la maison mère n'avaient eu connaissance du transfert de ces droits d'accès.

Dès que la société d'audit a indiqué que les droits d'administrateur pour le serveur et le pare-feu avaient été transférés à des collaborateurs du département informatique du Groupe X._____, la succursale a rapidement adopté les mesures nécessaires afin de reprendre le contrôle desdits droits. Elle a par ailleurs mandaté une société d'audit indépendante pour que celle-ci lui apporte les conseils nécessaires à sa mise en conformité. X._____ SA a ultérieurement engagé d'autres mesures qu'elle a partiellement mises en œuvre.

Extrait des considérants

(…)

2. Qualité de partie de X._____ SA

(28) X._____ SA est une succursale de banque étrangère au sens de l'article 2 al. 1 let. a de l'ordonnance de la FINMA sur les banques étrangères (OBE-FINMA ; RS 952.111) ainsi qu'une succursale de négociant étranger au sens de l'art 39 al. 1 let a ch. 1 de l'ordonnance sur les bourses (OBVM ; RS 954.111). En tant que succursale, X._____ SA fait juridiquement partie du Groupe X._____ et n'a pas de personnalité juridique propre selon le droit civil. Du point de vue du droit de surveillance, la succursale fait l'objet d'une surveillance consolidée de l'autorité du siège (…). Elle est cependant également au bénéfice d'autorisations délivrées par l'autorité de surveillance suisse à sa maison mère pour exercer son activité bancaire et de négociant en Suisse et il appartient dès lors à la FINMA de vérifier que les conditions afférentes à ces autorisations sont respectées en tout temps. Lors de la création d'une succursale en Suisse, la maison mère à l'étranger est responsable de la mise en place d'une organisation adéquate ainsi que de l'apport de ressources financières et en personnel suffisantes pour pouvoir obtenir une autorisation de la FINMA. Une fois l'entité créée et l'exercice de l'activité assujettie débuté, la succursale bénéficie d'une certaine autonomie et c'est à elle qu'il revient avant tout de remplir les obligations découlant du droit suisse de surveillance. Ainsi, ce sont les organes de la succursale qui doivent présenter toutes les garanties d'une activité irréprochable selon le droit suisse et peuvent faire l'objet de mesures de la FINMA (art. 4 al.1 let. g OBE-FINMA) à l'exclusion de ceux de la maison mère (cf. Bulletin CFB 45, p. 111). De même, ce sont principalement les organes et employés de la succursale suisse qui sont soumis au secret bancaire ou professionnel découlant des art. 47 LB et 43 LBVM (cf. infra, ch. 30 et ss.). Par conséquent, il y a lieu de considérer que les succursales de banques ou négociants étrangers, une fois débutées leur activité en Suisse, sont des assujettis au sens de l'art. 3

de la loi sur l'Autorité fédérale des marchés financiers (LFINMA ; RS 956.1). La présente décision est dès lors dirigée contre X._____ SA. Une copie de cette décision sera toutefois adressée au Groupe X._____ ainsi qu'à la Commission de surveillance du secteur financier (CSSF), chargée de la surveillance consolidée.

3. Législation applicable aux succursales suisses de banques ou de négociants étrangers

(29) Les dispositions de la loi sur les banques (hormis les art. 4 et 4bis LB en matière de fonds propres et de répartition des risques) et de la loi sur les bourses ainsi que de leurs ordonnances d'application sont applicables aux activités exercées en Suisse par des banques ou négociants étrangers (art. 2 al. 1 de la loi sur les banques [LB ; RS 952.0], 3 al. 1 OBE-FINMA et 40 al. 1 OBVM).

(…)

5. Exigence d'une organisation adéquate et outsourcing informatique

(33) Pour pouvoir obtenir et conserver l'autorisation d'exercer une activité en Suisse, les succursales de banques et de négociants étrangers doivent respecter en permanence les conditions d'autorisation fixées aux art. 4 OBE-FINMA, 3 al. 2 let. c et d ainsi que 3bis al. 1 LB, de même que 41 OBVM. Parmi ces conditions, figure en particulier celle d'une organisation adéquate découlant de l'exigence générale contenue à l'art. 3 al. 2 let. a LB, laquelle est concrétisée pour les succursales de banques et de négociants étrangers aux art. 4 al. 1 let. a OBE-FINMA et 41 al. 1 let. a OBVM. En vertu de ces dernières dispositions, une banque étrangère ou un négociant étranger doit disposer d'une organisation adéquate ainsi que du personnel qualifié nécessaire pour pouvoir exploiter une succursale en Suisse. La succursale doit être organisée en fonction de son activité et disposer d'un règlement définissant exactement son champ d'activité et prévoyant une organisation administrative correspondant à cette activité (art. 4 al. 1 let. g OBE-FINMA et art. 41 al. 1 let f OBVM). Les risques (notamment opérationnels, juridiques et réputationnels) doivent être déterminés, limités et contrôlés par la succursale (art. 9 al. 2 OB ainsi que art. 19 al. 3 OBVM ; cf. Bulletin CFB 45 p. 111 et ss.). L'établissement doit par ailleurs veiller à ce qu'il existe un système de contrôle interne efficace (art. 9 al. 4 OB et 20 al. 1 OBVM). Par contrôle interne, on entend l'ensemble des structures et processus de contrôle qui, à tous les échelons de l'établissement, constituent la base de son bon fonctionnement et la réalisation des objectifs de la politique commerciale. Le contrôle interne ne comprend pas uniquement les activités de contrôle a posteriori, mais également celles en rapport avec la gestion et la planification. Le contrôle des risques ainsi que la compliance font partie des fonctions clés d'un système de contrôle interne efficace (cf. Circ.-FINMA 2008/24 « Surveillance et contrôle interne » Cm 2).

(34) La Circulaire FINMA 2008/7 « Outsourcing – banques » précise quelles sont les mesures organisationnelles devant être adoptées par un établissement afin de garantir la protection des données de clients et le secret bancaire lors de l'externalisation de certaines prestations (outsourcing). Lorsqu'une succursale de banque ou de négociant étrangers externalise des prestations de services essentielles à son activité auprès de son siège à l'étranger, elle doit notamment respecter les principes 5 et 6 de cette circulaire (Circ.-FINMA 2008/7 Cm 6 et 7). Sont notamment considérées comme des prestations essentielles certains services en lien avec les systèmes de technologie de l'information et leur entretien, tels que le stockage de données, l'exploitation et l'entretien de banques de données ainsi que l'exploitation de systèmes de technologie de l'information (annexe à la Circ.-FINMA 2008/7 Cm 5). Lors de délégation de tels services à l'étranger, il doit être garanti, par des moyens techniques et organisationnels appropriés, que le secret bancaire et la protection des données des clients seront respectés conformément au droit suisse (principe 5 de la Circ.-FINMA 2008/7 Cm 35). Les clients doivent en outre être informés de

l'externalisation avant que des données les concernant soient transmises à un délégataire. Avant le transfert à l'étranger de données les concernant, une information détaillée doit être adressée aux clients par courrier spécial et ceux-ci doivent être informés des mesures de sécurité prises à cet effet et avoir la possibilité de mettre fin aux relations contractuelles dans un délai approprié avant un tel transfert (principe 6 de la Circ.-FINMA 2008/7 Cm 37 à 39).

(35) En l'espèce, X._____ SA a externalisé en 2005 les opérations informatiques et la gestion de son application bancaire auprès de son siège (…). D'un point de vue formel, le Service Level Agreement conclu en 2007 entre X._____ SA et le Groupe X._____ (paragraphe 4.8 du SLA) au sujet de cette externalisation prévoit expressément que les données de clients de la succursale suisse doivent être maintenues dans une base de données séparée à (…) et que l'accès au serveur de X._____ SA est protégé par un pare-feu administré par la succursale suisse pour garantir le secret bancaire.

(36) Après le départ d'un membre de sa direction, fin mars 2009, X._____ SA ne s'est toutefois pas préoccupé de savoir qui allait désormais assurer l'administration des serveurs contenant les données confidentielles des clients de la succursale suisse ainsi que du pare-feu de X._____ SA, alors que cette personne était pourtant expressément chargée de la liaison avec les services informatiques du siège. X._____ SA a déclaré à la FINMA n'avoir pas été informée par les informaticiens du siège que ceux-ci avaient décidé de reprendre les droits d'administrateurs sur le serveur et le pare-feu de X._____ SA. Il est toutefois critiquable que X._____ SA ne se soit pas informée du contenu et de l'étendue des travaux informatiques effectués par le service informatique du siège lorsque ce dernier a désinstallé, au printemps 2009, la console de gestion du pare-feu dans les locaux de la succursale suisse. X._____ SA n'a par ailleurs pris aucune mesure préventive ou de contrôle afin s'assurer et de vérifier, ou de faire vérifier par un tiers, que les moyens techniques en place auprès de la succursale permettaient toujours de garantir le secret bancaire et la protection des données des clients de X._____ SA. L'origine de ce désintérêt est à rechercher dans le fait qu'aucun des organes et collaborateurs de la succursale suisse ne disposait des connaissances informatiques suffisantes.

(37) Sur la base des éléments qui précèdent, il apparaît que X._____ SA a violé le principe 5 de la Circulaire FINMA 2008/7 de même que le paragraphe 4.8.2 du Service Level Agreement conclu avec son siège en ne garantissant pas le secret bancaire et la protection des données de ses clients vis-à-vis de sa maison mère par des moyens appropriés entre avril et novembre 2009. En outre, bien que l'externalisation des opérations informatiques et de la gestion de l'application bancaire remonte à 2005, ce n'est qu'en juin 2009, après plusieurs recommandations de PWC, que la succursale a finalement entrepris de modifier ses conditions générales afin d'informer les clients de cet outsourcing, puis de rédiger, en juillet 2010 seulement, un projet de lettre d'information à sa clientèle. Cela étant, X._____ SA a violé le devoir d'information dû à sa clientèle concrétisé au principe 6 de la Circulaire FINMA 2008/7.

(38) X._____ SA n'a par ailleurs pas adopté toutes les mesures nécessaires au sens de l'art. 9 al. 2 OB afin de limiter et contrôler les risques opérationnels, juridiques et réputationnels découlant de l'externalisation de ses opérations informatiques auprès de son siège (…). Il apparaît également que le système de contrôle interne de la succursale était défaillant, en violation de l'art. 9 al. 4 OB, puisqu'il n'a pas permis de détecter l'irrégularité relative aux droits d'administration sur le serveur et le pare-feu de la succursale avant l'intervention de PWC en novembre 2009 (art. 9 al. 4 OB et art. 20 al. 1 OBVM).

(39) En conclusion, X._____ SA ne disposait donc pas d'une organisation adéquate correspondant à son modèle d'activité, en tant que

succursale de banque et négociant étranger externalisant des prestations de services essentielles auprès de son siège, et ce faisant, la succursale a gravement violé les conditions d'autorisations fixées aux art. 4 al. 1 let. a OBE-FINMA et 41 al. 1 let. a OBVM.

6. Mesures à adopter par la FINMA

(40) Suite à la découverte par PWC de l'irrégularité liée aux droits d'administration accordés à des collaborateurs du siège sur le serveur et pare-feu de la succursale suisse, X._____ SA a immédiatement adopté les mesures nécessaires afin de reprendre le contrôle du pare-feu et du serveur et de supprimer l'irrégularité constatée par la société d'audit. Sur le plan organisationnel, un comité d'outsourcing comprenant des membres de la direction de la succursale et du siège a été mis en place par la banque. Les collaborateurs de X._____ SA ont en outre été formés afin d'assurer la gestion du pare-feu de la succursale. Enfin, la formation des informaticiens du siège a été renforcée en matière de sécurité de l'information et ceux-ci ont bénéficié d'un cours sur l'application de la Circulaire FINMA 2008/7 « Outsourcing » et le secret bancaire suisse. X._____ SA a par ailleurs annoncé qu'elle était en train de modifier son règlement interne afin d'assurer qu'en cas de changement de fonction, les attributions d'un collaborateur quittant la banque ne puissent être dévolues à une autre personne sans l'aval de la direction de la succursale.

(41) Au vu des démarches déjà entreprises par la banque pour régulariser sa situation, il n'apparaît pas que la FINMA doive adopter des mesures complémentaires afin de rétablir l'ordre légal.

(42) Les violations des principes 5 et 6 de la Circulaire FINMA 2008/7 « Outsourcing » de même que les lacunes organisationnelles ainsi que celles liées à la gestion des risques et au système de contrôle défaillant de la succursale suisse ont toutefois exposé, pendant près de huit mois, les clients de la succursale suisse (…) à un risque d'accès indu à des données confidentielles les concernant. Cela étant, les violations commises doivent être qualifiées de graves et il se justifie dès lors de rendre une décision en constatation à l'encontre de X._____ SA au sens de l'art. 32 LFINMA.

(43) Dans la mesure où aucun indice d'accès effectif depuis le siège à l'étranger à des données confidentielles de clients de X._____ SA n'a été constaté et puisqu'il n'existe pas d'éléments démontrant une éventuelle révélation ou transmission d'informations confidentielles concernant des clients de X._____ SA au sens des art. 47 LB et 43 LBVM, il ne se justifie pas d'adopter d'autres mesures complémentaires en lien avec le secret bancaire ou professionnel.

(…)

Dispositif