CHAMBRE DES COMMUNES
HOUSE OF COMMONS
CANADA

Comité permanent de l'accès à l'information, de la protection des renseignements personnels et de l'éthique

ETHI • NUMÉRO 025 • 2e SESSION • 41e LÉGISLATURE

TÉMOIGNAGES

Le jeudi 29 mai 2014

Président

M. Pat Martin

Comité permanent de l'accès à l'information, de la protection des renseignements personnels et de l'éthique

Le jeudi 29 mai 2014

● (1105)

[*Traduction*]

Le président (M. Pat Martin (Winnipeg-Centre, NPD)): Bonjour, mesdames et messieurs. La présente séance du Comité permanent de l'accès à l'information, de la protection des renseignements personnels et de l'éthique est ouverte.

Monsieur Ravignat, avez-vous quelque chose à dire?

M. Mathieu Ravignat (Pontiac, NPD): Monsieur le président, avant que nous n'entreprenions nos travaux, je veux mentionner que, si j'ai bien compris, un renvoi particulièrement important a été fait au comité, de sorte que l'opposition tient à soumettre l'avis de motions suivant:

> Que, conformément au paragraphe 111.1(1) du Règlement, et sous réserve de l'ordre de renvoi du 28 mai 2014, le comité entreprenne une étude d'une durée d'au moins quatre séances concernant toutes les questions liées à la nomination proposée de Daniel Therrien au poste de commissaire à la protection de la vie privée du Canada; qu'il invite Daniel Therrien à se présenter devant lui; et qu'il rédige un rapport contenant ses conclusions et ses recommandations à l'intention de la Chambre.

J'aimerais vous communiquer deux autres avis que j'estime importants:

> Que le comité invite l'ancienne commissaire à la protection de la vie privée du Canada, Jennifer Stoddart, et la commissaire à la protection de la vie privée du Canada par interim, Chantal Bernier, à contribuer à son étude sur la nomination proposée de Daniel Therrien au poste de commissaire à la protection de la vie privée du Canada.
>
> Que le comité invite des experts en matière juridique et constitutionnelle et des spécialistes des questions relatives à la protection de la vie privée à lui présenter des témoignages concernant la nomination proposée de Daniel Therrien au poste de commissaire à la protection de la vie privée du Canada.

Chaque fois que nous avons affaire à un renvoi au comité de cette nature, il est crucial que le comité l'étudie.

Merci beaucoup.

Le président: Monsieur Ravignat, je suis désolé de vous interrompre, mais je dois vous dire que votre avis de motion n'est pas sujet à débat. Vous nous avez présenté vos avis de motion, et nous vous en remercions.

Monsieur Calandra.

M. Paul Calandra (Oak Ridges—Markham, PCC): Je ne vois pas d'inconvénient à ce que l'on tienne un bref débat à ce sujet.

Le président: Si le comité souhaite que l'on discute de la motion...

M. Paul Calandra: À tout le moins l'une de celles qui ont été proposées.

Le président: Trois motions distinctes ont été présentées. Est-ce que les membres du comité sont d'accord pour que l'on discute brièvement de l'une ou l'autre de ces motions? Si nous nous engageons dans cette voie...

M. Paul Calandra: À coup sûr, cela ne me dérange pas que l'on discute de l'une des motions concernant M. Therrien. Je vais me préparer à modifier les suggestions de M. Ravignat.

Le président: Les membres du parti ministériel ont avisé plus tôt la présidence de leur intention d'inviter ou d'assigner à comparaître devant lui M. Therrien, qui a été nommé au poste de commissaire à la protection de la vie privée, dont la nomination doit être examinée conformément à l'ordre de renvoi que M. Ravignat a mentionné dans son avis de motion.

Je ne veux pas que nous nous lancions dans un débat là-dessus à ce moment-ci.

M. Paul Calandra: Nous avons des témoins à entendre.

Le président: Nous allons manquer de temps. La séance sera probablement écourtée. En effet, nous risquons d'être interrompu par les cloches qui annonceront la tenue d'un vote sur un certain nombre de questions de nature procédurale qui sera tenu à la Chambre des communes. Nous devons donc utiliser le temps dont nous disposons de la façon la plus efficiente possible.

Par conséquent, j'aimerais à présent souhaiter la bienvenue aux témoins que nous accueillons aujourd'hui dans le cadre de notre étude sur le problème grandissant du vol d'identité et ses répercussions économiques. Nous sommes très heureux de recevoir des représentants de cinq des principales banques à charte du Canada. Je vais les présenter dans l'ordre dans lequel ils ont demandé de prendre la parole. Ils nous présenteront à tour de rôle de brèves observations préliminaires, et ils répondront ensuite aux questions des membres du comité.

De la Banque Canadienne Impériale de Commerce, nous accueillons M. Philip Fisher, directeur senior, Gestion des risques des canaux électroniques. Bienvenue, monsieur Fisher. Nous entendrons ensuite M. Paul Milkman, vice-président senior, chef de la Gestion du risque technologique et de la Sécurité des systèmes d'information du Groupe Financier Banque TD. Soyez le bienvenu, monsieur Milkman. Nous recevons également M. Ed Rosenberg, vice-président et chef de la sécurité, Groupe légal, corporatif et de conformité, BMO Groupe financier. Nous vous souhaitons la bienvenue, monsieur Rosenberg. Jay Stark, vice-président, Services de vérification interne, Services bancaires aux particuliers et aux entreprises de la Banque Royale du Canada est également parmi nous. Bienvenue. Enfin, nous entendrons Jennifer Frook, directrice, Services partagés, Bureau de la gestion des fraudes.

Je suis très heureux que vous soyez tous parmi nous aujourd'hui. Nous aimerions profiter au maximum du temps dont nous disposons pour discuter du problème pressant qui fait l'objet de l'étude du comité. Je vous demande donc de procéder sans plus tarder dans l'ordre que j'ai mentionné, en commençant par M. Fisher, de la CIBC.

M. Philip Fisher (directeur sénior. Gestion des risques des canaux électroniques, Services intégrés de contrôle des affaires, Banque Canadienne Impériale de Commerce): Bonjour. Je m'appelle Philip Fisher, et je suis directeur senior, Gestion des risques des canaux électroniques de la CIBC. Je fais partie du groupe mis sur pied par notre organisation afin de se pencher sur les fraudes dont font l'objet les banques de détail. Je me spécialise plus particulièrement dans les questions liées à la criminalité en ligne ou, si l'on préfère, à la cybercriminalité, mais je suis en mesure de m'exprimer sur une vaste gamme de questions touchant la fraude.

J'aimerais d'abord et avant tout vous remercier, au nom de la CIBC, de me donner l'occasion de m'adresser à vous aujourd'hui et de répondre à toutes vos questions. J'aimerais également féliciter le comité d'avoir eu la volonté d'entreprendre une étude sur une question aussi importante pour notre industrie et pour une multitude de Canadiens qui sont touchés chaque jour par le vol d'identité. Il s'agit d'un sujet complexe, et nous vous sommes reconnaissants d'avoir pris l'initiative de vous pencher là-dessus.

Selon la CIBC, le vol d'identité est non pas un problème nouveau ou grandissant, mais plutôt une réalité en constante évolution. Le vol d'identité est un type de fraude qui existe depuis un certain temps. En revanche, les méthodes utilisées pour commettre ce crime ont changé. Il y a de cela un certain nombre d'années, il était question de vols de reçus, de factures ou de portefeuille, ou alors de fraudes par téléphone. À présent, il est question de menaces persistantes avancées, d'atteintes aux dispositifs de sécurité des commerçants, de logiciels malveillants et de hammeçonnage. Les percées technologiques et la diffusion connexe de renseignements personnels sur Internet ont modifié le contexte de risque.

Afin de faciliter notre discussion d'aujourd'hui, je crois qu'il est important que nous nous entendions sur une définition du vol d'identité. D'après le Code criminel du Canada, quiconque obtient ou a en sa possession des renseignements identificateurs sur une autre personne en vue de commettre un acte criminel commet un vol d'identité. Quant aux renseignements identificateurs, ils comprennent notamment le nom d'une personne, son adresse, sa date de naissance, sa signature manuscrite ou électronique, son code d'usager, son numéro de carte de crédit ou de débit, son numéro de compte d'une institution financière, son numéro d'assurance sociale ou de permis de conduire ou l'un de ses mots de passe.

En règle générale, les institutions financières utilisent une définition plus restreinte du vol d'identité et ont tendance à surveiller et à déclarer les fraudes en fonction de leur type. Avant de vous fournir de plus amples renseignements concernant ces divers types de fraude, je tiens à souligner que les institutions financières ne se servent pas toutes d'une définition commune du vol d'identité. Il s'agit là de l'une des raisons pour lesquelles il est difficile d'obtenir des données globales sur le phénomène.

Comme je viens de le dire, les types de fraude sont généralement définis en fonction de la source des renseignements subtilisés ou de la manière dont ils sont utilisés. Parmi les divers types de fraude, mentionnons la copie à un point de vente ou à un guichet automatique de données contenues dans une carte à bande magnétique. Ceux qui obtiennent des renseignements de cette façon les utilisent habituellement pour créer des cartes de contrefaçon ou pour faire des achats au moyen de transactions sans carte. De façon générale, les banques estiment que ce type de fraude n'est pas assimilable à un vol d'identité en raison du nombre limité de renseignements ayant été volés. Le vol de renseignements contenus dans un ordinateur personnel infecté par un logiciel malveillant représente un type de fraude préoccupant en raison du nombre de renseignements en cause et de la difficulté que pose le fait de déceler et de régler le problème.

La fraude par courriel ou le hammeçonnage visant l'obtention de renseignements personnels est un type de fraude qui est en train d'évoluer. La tentative classique de hammeçonnage vise à obtenir des renseignements permettant d'accéder à un compte bancaire en ligne, par exemple un authentifiant ou un numéro de carte de crédit. Toutefois, on constate que les fraudeurs tentent de plus en plus d'élargir la gamme de renseignements à obtenir.

Il y a d'autres exemples de fraude, par exemple le vol de courriels ou les atteintes à la protection des données de tierces parties, notamment les commerçants et les fournisseurs de services de traitement des transactions. Comme l'ont montré des reportages récemment parus dans les médias, ces atteintes peuvent toucher un grand nombre de consommateurs, en fonction du commerçant visé par l'attaque. Un vol de portefeuille constitue un simple exemple de renseignements qu'un consommateur peut perdre ou se faire voler, mais ces renseignements peuvent aussi se faire voler après que le consommateur les a fournis à une tierce partie ou s'ils sont éliminés de façon inappropriée.

Quelques-uns de ces problèmes existent depuis un certain temps, et des mesures de contrôle solides et bien établies ont été mises en place afin de les déceler et de les régler. Par contre, certains de ces problèmes sont d'apparition plus récente, et les mesures de contrôle visant à les prendre en charge continuent d'évoluer. Quelques-uns de mes pairs aborderont cette question de façon plus approfondie durant leur exposé.

Même si elles se sont dotées de dispositifs perfectionnés de détection et de contrôle de la fraude, les institutions financières ne parviendront pas seules à venir à bout du vol d'identité. Une lutte efficace contre ce problème passe par une initiative coordonnée des institutions financières, des consommateurs et du gouvernement. Les consommateurs jouent un rôle important au moment de se protéger eux-mêmes contre le vol d'identité — ils connaissent leurs renseignements personnels et la manière dont ils les utilisent, et ils sont donc les mieux à même de déceler toute utilisation non autorisée qui en est faite.

Cela dit, les consommateurs ne sont pas des spécialistes de la fraude, et ils ont besoin d'orientation et de soutien. Les institutions financières et les organismes gouvernementaux offrent aux consommateurs un soutien essentiel en les informant à propos des risques et en leur fournissant des outils leur permettant de se protéger eux-mêmes. Certains services qu'offrent des institutions financières, notamment l'envoi d'alertes en cas de transaction douteuse ou la surveillance gratuite d'une agence d'évaluation du crédit, constituent de bons exemples d'outils que les consommateurs peuvent utiliser. L'un de mes collègues vous en dira plus long à ce sujet durant son exposé.

On ne saurait sous-estimer l'importance du rôle que joue le gouvernement en matière de protection des consommateurs contre le vol d'identité. Comme je l'ai expliqué plus tôt, en raison de l'évolution de la technologie, notre environnement change de façon rapide et substantielle. Des dispositions législatives adéquates s'assortissant de conséquences appropriées ont un puissant effet dissuasif sur ceux qui songent à commettre un vol d'identité. Dans le passé, les institutions financières ont prôné l'adoption de dispositions législatives touchant le vol d'identité. Elles continueront de soutenir le gouvernement au moment où il tentera de renforcer les mesures de contrôle dans ce domaine en constante évolution.

● (1110)

Dans le cadre de mon travail, j'ai pu constater par moi-même qu'un tel partenariat peut fonctionner. La copie de renseignements contenus dans les cartes bancaires au moyen du trafiquage de guichets automatiques est une activité qui a énormément évolué au fil des ans.

Lorsque j'ai commencé à étudier la question, la CIBC comptait par centaines les cas de trafiquage de guichets automatiques. À présent, grâce au dispositif inviolable dont sont dotés les guichets automatiques et au fait que ceux qui commettent un tel crime sont plus susceptibles d'être envoyés en prison, les incidents de cette nature peuvent se compter sur les doigts d'une main. D'autres institutions bancaires qui ont pris des mesures semblables ont pu constater la même chose. Nous nous réjouissons à l'idée de prendre des mesures aussi fructueuses à d'autres égards.

En terminant, je tiens à remercier de nouveau les membres du comité de m'avoir donné l'occasion de m'adresser à eux sur cette question importante, et je serai heureux de répondre à toutes les questions qu'ils voudront bien me poser.

Le président: Merci beaucoup, monsieur Fisher.

Le prochain intervenant sera M. Paul Milkman du Groupe financier Banque TD.

● (1115)

M. Paul Milkman (vice-président sénior, Chef de la Gestion du risque technologique et de la Sécurité des systèmes d'information, Groupe Financier Banque TD): Je vous remercie, monsieur le président, de me donner l'occasion d'être ici aujourd'hui.

Comme je suis Américain et que je ne vis au Canada que depuis cinq ans, il s'agit de la première fois que j'ai l'occasion de me présenter devant un comité parlementaire canadien, et je suis très heureux qu'on m'ait offert cette possibilité.

[*Français*]

Je suis désolé de ne pas pouvoir m'exprimer en français, mais je suis Américain.

[*Traduction*]

Je crois que Philip a très bien établi les paramètres d'une réflexion concernant le vol d'identité.

Le vol d'identité est un crime. L'utilisation active d'une identité volée aux fins de la perpétration d'une fraude de nature financière constitue un acte et un crime distincts. Toutefois, les banques doivent disposer de stratégies de prévention intégrées puisqu'il peut y avoir une relation de cause à effet entre un vol d'identité et une fraude financière. J'aimerais également souligner que, en ce qui concerne tant le vol d'identité que la fraude, les intérêts des banques sont étroitement liés à ceux de leurs clients. Les banques font tout ce qu'elles peuvent pour empêcher que leurs clients soient victime de l'un de ces crimes.

De quelle façon envisageons-nous la prévention? Nous estimons qu'il s'agit d'un domaine où les responsabilités doivent être partagées entre les banques et leur clientèle, qui doivent toutes deux faire preuve de vigilance. La Banque TD a mis en place un processus en quatre étapes pour s'assurer que ses clients prennent des mesures responsables en vue de protéger leurs renseignements personnels. Si vous le permettez, je vais décrire brièvement chacune de ces étapes.

Premièrement, nous demandons à nos clients de faire preuve de prudence au moment de communiquer leurs renseignements personnels. Nous leur recommandons de poser des questions à ceux qui leur demandent de tels renseignements quant à la façon dont ils seront utilisés, la raison pour laquelle ils doivent être fournis, les personnes auxquelles elles seront transmises et les mesures qui seront prises afin d'en préserver la confidentialité. Il ne faut jamais divulguer son numéro d'identification personnel, son numéro d'assurance sociale ou un quelconque mot de passe. En outre, on ne doit pas se servir dans les médias sociaux de mots de passe utilisés aux fins de transactions bancaires.

Deuxièmement, nous demandons à nos clients de prendre des mesures de sécurité appropriées. Les gens doivent conserver en lieu sûr leurs relevés de compte, vu qu'ils contiennent des renseignements personnels et de nature délicate. Ils doivent tirer parti des technologies qui leur permettent de naviguer sur Internet de façon plus sécuritaire et en protégeant mieux leurs renseignements personnels. Ces technologies comprennent notamment les signatures numériques, les logiciels antivirus, les pare-feu personnels et le cryptage des données. Par exemple, TD offre à ses clients un téléchargement gratuit du logiciel Trusteer Rapport, qui prévient le hammeçonnage et certaines attaques de logiciel malveillant touchant le navigateur des ordinateurs infectés. TD leur offre également un abonnement de un an au logiciel antivirus McAfee. Nous offrons gratuitement ces outils à nos clients afin de les aider à se protéger eux-mêmes non seulement lorsqu'ils effectuent des transactions bancaires, mais également dans le cadre de toute utilisation qu'ils font d'Internet.

Troisièmement, ils doivent vérifier l'exactitude de leurs relevés de compte. Ils doivent s'assurer que toutes les transactions et tous les frais qui y figurent sont exacts. Nous leur recommandons aussi d'obtenir une fois par année un rapport de solvabilité d'une agence d'évaluation du crédit comme Equifax ou TransUnion pour s'assurer que tout est en ordre à ce chapitre.

Quatrièmement, ils doivent protéger leurs cartes, leurs chèques et leurs cartes d'identité. Nous leur conseillons de n'apporter avec eux en voyage que les cartes de crédit dont ils ont besoin, de laisser à la maison leur carte d'assurance sociale et d'entreposer en lieu sûr une liste de toutes leurs cartes et des numéros connexes.

Ces mesures les aideront à se prémunir contre le vol d'identité et contre toute fraude pouvant en découler.

Comme je l'ai indiqué, la prévention est une responsabilité partagée, et les banques doivent, pour leur part, indiquer clairement les renseignements personnels qu'elles conservent à propos d'un client, la procédure qu'un client doit utiliser pour y accéder, et surtout, les mesures qu'elles prennent pour assurer la protection de ces renseignements personnels.

En ce qui concerne la conservation de renseignements personnels, je vous dirai que les banques utilisent de tels renseignements afin d'établir l'identité de leurs clients. Afin d'offrir des produits et des services à nos clients ou pour les protéger contre le blanchiment d'argent ou d'autres types d'opération, nous avons besoin d'obtenir diverses informations à leur sujet, notamment leur nom, leur adresse, leur date de naissance, leur emploi et d'autres renseignements liés à leur identité. Il se peut que nous devions obtenir d'autres renseignements personnels afin de leur offrir certains produits, par exemple un prêt hypothécaire. Nous pouvons également demander à des tierces parties, notamment des agences d'évaluation du crédit, de nous transmettre de l'information à leur sujet, mais nous ne le faisons qu'avec le consentement du client.

Les clients peuvent en tout temps accéder aux renseignements que leur banque possède à leur sujet ou les mettre à jour. En outre, plusieurs options relatives à la protection de leur vie privée leur sont offertes; Par exemple, ils peuvent indiquer qu'ils ne veulent pas que des agences de marketing direct communiquent avec eux ou choisir de ne pas participer à des sondages ou à des enquêtes auprès de la clientèle.

En ce qui a trait plus précisément à la protection des renseignements personnels des clients, je mentionnerai que les banques investissent des sommes substantielles afin de répondre continuellement à des normes élevées en matière de sécurité et de protéger leurs systèmes et les renseignements personnels de leurs clients contre toute consultation ou utilisation non autorisée. Par exemple, nos systèmes ont été conçus pour préserver en tout temps le caractère privé et confidentiel des numéros d'identification personnels, des mots de passe et des autres codes d'accès. À des fins de protection, seuls les clients connaissent leur code d'accès — nos employés ne peuvent pas les obtenir ni demander aux clients de les leur fournir. En outre, tous les fournisseurs et les agents avec lesquels TD fait affaire se sont engagés à préserver la confidentialité des renseignements de nos clients, et ils ne peuvent pas les utiliser à des fins non autorisées. De surcroît, ils doivent prouver que, dans le cadre de leurs activités, ils utilisent des dispositifs appropriés de contrôle et de protection.

● (1120)

Les banques ont pris des mesures particulières en ce qui concerne l'environnement en ligne. À ce chapitre, TD a notamment pris des mesures touchant la collecte de renseignements exhaustifs sur les menaces, la mise en place de dispositifs de contrôle de gestion de l'accès, la journalisation et l'analyse des transactions, la mise en place de pare-feu sécurisés, la surveillance continue visant la détection proactive des activités inhabituelles dans les comptes des clients, la protection contre le hammeçonnage et les pourriels et l'adoption des logiciels de cryptage les plus perfectionnés pour faire en sorte que les données ne puissent être décodées et déchiffrées que par notre système ou le client concerné.

En conclusion, je vous dirai que les banques et leurs clients seront toujours préoccupés par ces deux problèmes jumeaux que représentent le vol d'identité et la fraude financière. Nous devrons toujours lutter contre les criminels qui veulent voler des données et les utiliser à leur profit, mais pour ce qui est de la gestion des risques en matière de technologies de l'information, je peux vous dire que les banques sous réglementation fédérale du Canada respectent les normes mondiales les plus élevées au chapitre de la sécurité des renseignements et de la protection contre le vol d'identité.

Merci.

Le président: Merci beaucoup, monsieur Milkman.

Nous allons tout de suite passer au prochain intervenant, à savoir M. Ed Rosenberg, de BMO Groupe financier.

M. Ed Rosenberg (vice-président et chef de la sécurité, Groupe légal, corporatif et de conformité, BMO Groupe financier): Bonjour, monsieur le président, et merci beaucoup.

Au nom de BMO Groupe financier, je suis très heureux de prendre part à la discussion d'aujourd'hui sur la question du vol d'identité, et plus précisément sur les moyens mis en oeuvre par le Canada afin de protéger nos clients, nos employés et nos actifs contre la fraude et les autres actes criminels.

Le moment est bien choisi pour prendre la parole ici aujourd'hui, si peu de temps après que ce soit terminé le Mois de prévention de la fraude, qui a eu lieu en mars. Au cours de ce mois, BMO s'est joint à d'autres institutions financières, à des groupes de défense des consommateurs, à des organismes chargés de l'application de la loi et à ses partenaires de l'Association des banquiers canadiens afin de sensibiliser les consommateurs à la fraude et à l'importance d'en réduire les occurrences.

BMO prend le vol d'identité et toutes les activités criminelles très au sérieux. Nous croyons que chacun de nos employés a un rôle important à jouer en vue de réduire les cas de fraude. Nos politiques d'entreprise ont pour objectif de prévenir et de détecter les activités criminelles potentielles et d'y donner suite. Les activités que nous menons dans le domaine de la sécurité commerciale sont le fruit de près de 200 années d'expérience — tout au long de notre histoire, nous avons protégé les renseignements de nos clients tout en leur permettant d'accéder facilement à leur compte.

La protection des renseignements de nos clients suppose que nous devons nous adapter à l'évolution et à la complexité des activités criminelles, par exemple la fraude, la corruption, la cybercriminalité et les actes de violence. En outre, nous expliquons clairement à l'ensemble de nos employés en quoi consistent leurs rôles et leurs responsabilités de manière à ce que les particuliers et leurs groupes d'affaires respectifs s'engagent fermement dans la gestion des risques liés aux activités criminelles.

Voilà deux mois à peine, nous avons organisé un certain nombre d'activités de sensibilisation. Par exemple, entre autres, nous avons tenu des séances d'information auprès des employés de notre entreprise sur la lutte contre la fraude, nous avons mis à la disposition de nos clients en succursale des dépliants sur le hammeçonnage, nous avons ajouté à nos relevés bancaires des conseils pour éviter la fraude et nous avons diffusé notre message sur Twitter et sur Facebook.

Nos employés, qui travaillent au sein de nos divers secteurs d'activité et qui occupent des postes allant de celui de préposé au service à la clientèle dans les succursales locales à celui de négociant en matières premières et en contrats à terme, constituent notre défense de première ligne dans le cadre de notre lutte contre la fraude. Nous travaillons avec eux à l'élaboration de programmes destinés à prévenir et à détecter les risques d'activité criminelle dans leurs secteurs de responsabilité, par exemple la gestion des contrôles internes sur le traitement des espèces, des dossiers de crédit et des transactions; la gestion des renseignements personnels et financiers de nos clients; ainsi que la surveillance et la conformité avec les exigences des organismes de réglementation.

L'environnement dans lequel notre entreprise évolue est en perpétuel mouvement. Nos processus et nos dispositifs de contrôle internes font l'objet d'importantes innovations. La réalité des risques que nous courons face à la criminalité change au quotidien, et les banques sont organisées pour faire face à cette situation. Nous essayons, par l'authentification, de valider les renseignements et les documents; toutefois, il se peut que la qualité et la sécurité des documents varient d'une administration à l'autre, et il existe peu de moyens fiables d'authentifier les documents de façon universelle.

Nous appliquons une politique de tolérance zéro à l'égard des activités criminelles, et nous avons adopté des pratiques qui nous aident à gérer la manière dont nous réagissons à toute activité susceptible de se produire.

Une partie des efforts que nous déployons vise à identifier les personnes qui se livrent à des activités de fraude financière. Notre industrie investit des millions de dollars pour prévenir et détecter les comportements criminels et lutter contre eux, et elle affecte des centaines d'employés à ces tâches. De plus, nous collaborons à des initiatives qui, dans certains cas, sont organisées par l'ensemble de l'industrie et menées sous l'égide de l'Association des banquiers canadiens, afin d'identifier les criminels et de collaborer avec les organismes d'application de la loi en vue de les poursuivre en justice.

Les banques disposent d'experts et de systèmes de sécurité extrêmement perfectionnés afin de protéger les renseignements de leurs clients et d'éviter de devenir elles-mêmes victimes d'une fraude financière. Comme je l'ai indiqué précédemment, chaque banque investit des sommes substantielles dans la détection des activités frauduleuses. L'adoption des normes en matière de cartes à puce et de numéros d'identification personnels a coûté à elle seule des millions de dollars à l'industrie, qui a fait ces investissements en vue de réduire les risques de fraude liés aux cartes au Canada.

Cependant, dans un environnement en constante évolution, le crime organisé se tourne de plus en plus vers de nouvelles technologies et exploite d'autres avenues. Les membres de l'industrie ont mis en place des forums de discussion et des outils de collaboration afin d'échanger des renseignements sur les tendances en matière de fraude et les mécanismes de contrôle préventif. Pour contribuer à protéger l'industrie, par le truchement de l'ABC et d'autres instances, nous entrons en communication avec une multitude d'intervenants, qu'il s'agisse de fournisseurs d'accès Internet dans le cas de la cybercriminalité, de compagnies d'assurance en ce qui a trait aux fraudes courantes ou d'organismes d'application de la loi pour ce qui est du partage de renseignements touchant les tendances.

Nous prenons également des mesures de ce genre à l'échelle internationale. Pas plus tard qu'il y a deux semaines, j'ai rencontré des pairs de plus de 30 banques de partout dans le monde afin de discuter avec eux des risques auxquels nous sommes confrontés, de la façon dont nous pouvons protéger nos institutions et nos clients et de la meilleure manière de collaborer ensemble et d'accroître l'ampleur de nos efforts.

Monsieur le président, il est évident que la protection des renseignements que vous, les membres du comité et moi-même considérons comme partie intégrante de notre identité numérique unique constitue un véritable travail d'équipe auquel doivent contribuer les personnes qui détiennent ces renseignements et les intervenants auxquels ils font confiance.

Chez BMO, nous sommes fiers de la solide capacité du secteur des services bancaires du Canada d'offrir à ses clients un accès sécuritaire et commode à leurs renseignements financiers.

Au nom de BMO, je tiens à vous dire que je suis très heureux d'être ici aujourd'hui, et que je me réjouis à l'idée de répondre à toute question que vous voudrez bien me poser.

● (1125)

Le président: Merci, monsieur Rosenberg.

Nous allons maintenant entendre le représentant de la RBC, à savoir M. Jay Stark, vice-président.

M. Jay Stark (vice-président, Services de vérification interne, Services bancaires aux particuliers et aux entreprises, RBC): Bonjour. Je m'appelle Jay Stark. Si je suis ici pour représenter la RBC, c'est parce que j'ai occupé pendant 11 ans le poste de vice-président des services de gestion de la fraude.

La RBC s'emploie à fournir à ses clients des services financiers sécuritaires. Nous pouvons nous enorgueillir d'une longue tradition d'innovation et d'excellence en matière de gestion de la fraude. Je vous remercie d'avoir invité la RBC à s'adresser à vous aujourd'hui. Nous félicitons le comité et le gouvernement de mener une étude sur le vol d'identité.

Le vol d'identité est un crime grave qui provoque des pertes financières substantielles, des désagréments considérables et un sentiment d'insécurité chez les consommateurs, en plus de permettre aux criminels de financer leurs activités et de dissimuler leur identité. De surcroît, le vol d'identité peut contribuer aux activités terroristes.

Vous avez entendu les témoignages de mes collègues et d'autres personnes qui se sont présentées devant vous. Vous avez pu constater que la définition du vol d'identité, tout comme celle de la fraude, varie selon les intervenants de l'industrie. Toutefois, tout le monde s'entend pour dire que le vol d'identité constitue un type important de crime de nature financière. Comme l'ont montré sans l'ombre d'un doute les recherches qui ont été menées et les témoignages qui vous ont été livrés, le vol d'identité est un sujet complexe. Les avis des intervenants divergent non seulement sur le nombre de cas de vols d'identité qui ont été commis ou sur la définition de ce crime, mais également sur les solutions à ce problème. Afin de réagir de façon prompte, efficace et efficiente, nous devons mettre en oeuvre un éventail de stratégies de lutte contre la fraude dans le cadre d'une démarche éprouvée. À mon avis, c'est à cet égard que mes collègues et moi sommes les mieux à même d'aider le comité.

Une démarche fructueuse doit optimiser les liens entre ce que j'appelle les quatre piliers de la gestion de la fraude. Ces piliers sont les suivants: les répercussions sur les clients ou les désagréments qui leur sont causés; les pertes liées aux fraudes; les coûts liés à la fraude que doivent assumer les banques et la société; et enfin, la gestion des risques.

Un cadre axé sur ce que l'on pourrait désigner comme la chaîne de valeur de la lutte contre la fraude doit établir un juste équilibre entre les divers éléments stratégiques clés de la gestion de la fraude, à savoir le renseignement, par exemple, l'utilisation de données négatives, l'établissement de liens entre les incidents de nature criminelle et la mise en commun d'information relative aux tendances et aux pratiques exemplaires; la prévention — laquelle englobe la sensibilisation et l'éducation des consommateurs, par exemple en ce qui a trait à l'utilisation des cartes à puce et des NIP; la détection — laquelle exige des analyses de pointe, des partenariats au sein de l'industrie et des enquêtes menant, entre autres, à des poursuites et à la récupération d'éléments d'actifs; et enfin l'analyse des causes profondes.

Chacun de ces éléments stratégiques de la lutte contre la fraude offre un rendement marginal décroissant. Par exemple, il est pratiquement impossible d'intenter une poursuite contre toutes les personnes ayant participé à un stratagème donné de fraude de carte de débit, et il ne serait pas réaliste de tenter de prévenir la fraude en réduisant à 10 $ la limite de retrait ou en bloquant les agences d'évaluation du crédit afin de dissuader les criminels. En outre les stratégies que nous utilisons donnent lieu à un déplacement des activités liées à la fraude. Par exemple, la mise en oeuvre des cartes à puce et des NIP s'est traduite par une augmentation substantielle des fraudes transfrontalières et des fraudes liées aux transactions sans carte.

Les initiatives de l'industrie et, surtout, les progrès réalisés au chapitre des analyses relatives à la détection, y compris le perfectionnement des techniques d'analyse et l'application de données plus solides sur les plans qualitatif et quantitatif, ont constitué les stratégies de lutte contre la fraude les plus efficaces de la dernière décennie. Conjuguées à d'autres éléments stratégiques, les analyses en vue de la détection ont permis d'obtenir des résultats différentiels et d'optimiser l'ensemble du programme de gestion de la fraude.

L'application de cette démarche et de ces stratégies à un vaste éventail de stratagèmes de fraude — notamment les fraudes liées aux prêts sur carte de débit ou de crédit et les fraudes liées aux chèques — a donné de très bons résultats. En fait, en dépit de la croissance de son portefeuille et du perfectionnement incessant des activités criminelles, la RBC a obtenu l'an dernier ces meilleurs résultats de la décennie en matière de fraude — le nombre absolu de cas de fraude par lesquels elle a été touchée a été le plus bas des 10 dernières années. La RBC consacre énormément de temps et de ressources à l'examen, à la mise à l'essai et à l'amélioration de ses stratégies de lutte contre les crimes de nature financière, y compris le vol d'identité.

Vu que le temps dont je dispose est malheureusement limité, je conclurai en mentionnant que nous serions heureux de collaborer avec le comité dans le cadre de son importante étude et de lui fournir toute aide supplémentaire dont il aura besoin pour la mener à bien. J'ai hâte d'entendre vos questions et vos observations, et je me réjouis à l'idée de collaborer avec vous dans l'avenir.

Je vous remercie de m'avoir donné l'occasion de m'adresser à vous.

Le président: Merci, monsieur Stark.

Enfin, la dernière intervenante, mais non la moindre, sera Jennifer Frook, directrice des Services partagés du Bureau de la gestion des fraudes de la Banque Scotia.

● (1130)

Mme Jennifer Frook (directrice, Services partagés, Bureau de la gestion des fraudes, Banque Scotia): Bonjour. Je m'appelle Jennifer Frook, et je suis directrice du Bureau de la gestion des fraudes de la Banque Scotia. À ce titre, je suis responsable de l'évaluation des fraudes et de la communication de renseignements relatifs aux risques de fraude à l'échelle de notre organisation d'envergure mondiale. Cette tâche englobe l'établissement proactif des pratiques et des technologies de prévention de la fraude permettant d'atténuer l'exposition de notre institution bancaire à des pertes découlant de la fraude. Notre capacité de prévenir la fraude et de protéger nos clients contre ce crime dépend dans une large mesure de notre collaboration avec d'autres intervenants. Je suis également l'actuelle présidente du groupe d'experts sur la fraude de l'ABC.

Je me réjouis d'avoir la possibilité de m'adresser au comité sur un sujet que nous prenons tous très au sérieux et qui a des répercussions directes sur nos clients, notre industrie et l'économie. Pour les banques, il s'agit d'une question cruciale, étant donné l'importance que revêtent la confidentialité et la sécurité pour les activités bancaires. Si nos clients n'ont pas la certitude que nous protégeons adéquatement leur identité et leurs renseignements personnels, nous ne pouvons pas jouer notre rôle.

Afin de traiter des questions liées au vol d'identité qui intéressent le comité, je consacrerai mes observations préliminaires à un certain nombre de points pertinents, à savoir la formation et l'éducation, la prévention, la détection et l'atténuation, et enfin la collaboration.

Pour notre institution, l'un des éléments importants de la prévention de la fraude tient au fait de veiller à ce que notre personnel soit dûment formé afin de protéger nos clients contre le vol d'identité et les autres formes de fraude. La Banque Scotia dispose de programmes de formation rigoureux à l'intention de ses employés qui entrent en relation avec la clientèle dans nos succursales et nos centres d'appel ou dans le cadre d'activités liées à la sécurité des cartes bancaires. À leur arrivée au sein de notre organisation, nos employés doivent participer à un programme de formation exhaustif, et prendre part chaque année à des cours de recyclage. Il est tout aussi important pour nous d'habiliter nos clients en leur transmettant de l'information qui peut les aider à protéger leurs renseignements et à s'assurer qu'ils sachent exactement quelles mesures ils doivent prendre chaque fois qu'ils ont des préoccupations en matière de sécurité.

Pour prévenir la fraude, nous avons pris un certain nombre de mesures de sécurité en vue de protéger l'intégrité des renseignements concernant nos clients. Je vais vous fournir plusieurs exemples.

Au Canada, l'ensemble des cartes de crédit pour la vente au détail et des cartes de débit actives que nous délivrons, de même que tous les guichets automatiques de la Banque Scotia, sont munis de la technologie de la carte à puce, laquelle contribue à renforcer la protection contre les pertes, le vol et la contrefaçon de cartes.

Nos cartes de débit sont dotées de la technologie Flash Interac, laquelle utilise des puces sécurisées afin de protéger les consommateurs contre divers types de fraude, par exemple le clonage et la contrefaçon. Bon nombre de nos cartes de crédit pour la vente au détail sont munies d'une technologie semblable, à savoir la fonctionnalité Visa payWave. En outre, grâce à notre service InfoAlertes, nous pouvons envoyer à nos clients des courriels ou des messages texte afin de leur offrir une protection supplémentaire et de les aider à surveiller l'activité dans leurs comptes.

Comme mes collègues le font au sein de leur institution respective, nous offrons nous aussi à nos clients un logiciel gratuit qui les aide à protéger leurs renseignements. Nous avons établi un partenariat avec McAfee en vue d'offrir à tous nos clients qui utilisent nos services électroniques un abonnement gratuit de 12 mois au logiciel antivirus de cette société, qui contribue à la protection des appareils de nos clients contre les virus en ligne et les menace de réseau. Nous leur offrons également le logiciel Trusteer Rapport, qui les aide à se protéger contre les logiciels malveillants.

Tous les réseaux que nous utilisons et tous les produits que nous offrons s'assortissent d'un certain nombre de dispositifs de contrôle permettant de détecter les activités suspectes. Ces dispositifs à multiples couches sont de nature dynamique. Toutes ces mesures ont pour but de permettre à nos véritables clients d'accéder à nos services et d'empêcher les fraudeurs de le faire.

Nous mettons continuellement à l'essai nos technologies et nos systèmes, et nous surveillons et examinons sans cesse les activités de notre clientèle afin de déceler tout comportement inhabituel ou suspect pouvant être assimilé à de la fraude.

Bien entendu, malgré tous les efforts que nous déployons, les authentifiants et les autres renseignements personnels de nos clients sont susceptibles de faire l'objet de vol. Lorsque les banques détectent de tels risques, elles prennent les mesures appropriées pour protéger leur clientèle et réduire au minimum les pertes. Par exemple, elles avisent leurs clients du fait que la sécurité de leur carte ou de leur compte a été compromise, elles bloquent l'authentifiant volé et, dans la mesure du possible, elles le remplacent, notamment en émettant une nouvelle carte de crédit ou en réinitialisant le mot de passe qu'utilise le client pour accéder à son compte par voie électronique.

Nous surveillons les mouvements sur les comptes de nos clients afin de relever les transactions suspectes ou frauduleuses. Nous mettons à jour les profils de nos clients en y inscrivant les vols d'identité dont ils ont été victimes de manière à ce que les employés de première ligne puissent appliquer notre politique améliorée de connaissance du client au moment d'authentifier nos clients et leur compte. Bien entendu, nous indemnisons nos clients pour leurs pertes, et nous le faisons intégralement.

De plus, les banques collaborent avec le commissaire à la protection de la vie privée et lui transmettent toute information concernant une atteinte importante ou systémique à la sécurité des renseignements personnels.

● (1135)

Le vol d'identité est un crime qui évolue rapidement et constamment. Nous faisons de notre mieux pour nous assurer d'être toujours en mesure d'y faire face en surveillant et en évaluant les fraudes qui en découlent et en élaborant continuellement de nouvelles mesures de protection.

Je dois également mentionner que nous devons collaborer avec d'autres intervenants afin de prendre en charge le vol d'identité, vu que ce crime est presque toujours commis à l'extérieur de l'environnement bancaire et échappe donc à l'emprise des banques. Nos propres activités internes de surveillance de la fraude nous permettent de recueillir des renseignements que nous transmettons à un certain nombre d'institutions et d'intervenants, par exemple Visa, American Express, Interac, des organismes d'application de la loi et l'ABC. Ces organisations compilent également de l'information transmise par d'autres institutions financières, et elles fournissent à l'industrie des paramètres et des points de repère à partir desquels nous pouvons évaluer la mesure dans laquelle nous parvenons à limiter les cas de fraude, dont un certain nombre sont attribuables à un vol quelconque de renseignements personnels d'un client. Par exemple, l'ABC a créé un groupe composé d'experts en matière de fraude qui doivent travailler en collaboration afin de prévenir la fraude et de mettre en commun des renseignements et des pratiques exemplaires.

Si vous le permettez, je terminerai là-dessus, non sans répéter une fois de plus que notre institution bancaire est résolue à faire tout en son pouvoir pour veiller à la sécurité des renseignements personnels et financiers de ses clients.

J'ai hâte de répondre à vos questions. Merci.

Le président: Merci, madame Frook.

Je remercie tous les témoins des exposés qu'ils nous ont présentés aujourd'hui.

Je vous rappelle qu'il demeure possible que la séance soit interrompue par les cloches annonçant la tenue de votes, de sorte que nous allons passer sans plus tarder à la période de questions.

L'opposition officielle, le NPD, s'occupera du premier tour.

Monsieur Ravignat, vous avez sept minutes.

M. Mathieu Ravignat: Je remercie les témoins de leur présence aujourd'hui.

Vos exposés me donnent l'impression que vous ne comprenez pas vraiment bien l'ampleur du problème ainsi que l'importance de votre rôle. Je pense que la plupart des Canadiens seraient d'accord pour dire que les banques ont un rôle crucial à jouer pour ce qui est de s'assurer que le vol d'identité ne se produit pas.

Nous avons entendu des chercheurs affirmer qu'ils avaient tenté de communiquer avec des banques afin d'obtenir des renseignements sur des cas de vol d'identité et sur les pratiques en vigueur dans vos établissements pour s'assurer que cela ne se produit pas. Ils ont obtenu peu de réponses, et très peu de données leur ont été communiquées.

Je comprends que vos entreprises sont à but lucratif et que vous devez faire attention pour être concurrentiels par rapport à vos compétiteurs, mais il me semble qu'une plus grande transparence, une plus grande ouverture et un meilleur accès aux cas de vol d'identité ainsi qu'à vos pratiques aideraient les chercheurs, de même que les parlementaires, à étudier un problème de plus en plus grave.

J'aimerais vous demander pourquoi vous ne communiquez pas ce type de renseignements aux universitaires. Si vous le faites, ce serait peut-être rassurant, et il serait intéressant de le savoir.

Si quelqu'un désire présenter son point de vue, sentez-vous à l'aise de le faire.

Le président: Si plus d'une personne veut répondre, veuillez donner des réponses courtes, car il ne nous reste que sept minutes pour les questions et les réponses.

M. Ed Rosenberg: Je vais répondre à la question. Merci beaucoup, monsieur.

Au nom de mes pairs, une des questions auxquelles nous sommes confrontés concerne les universitaires qui ont abordé les institutions. Aucun d'entre nous n'a pu déterminer à qui ils s'étaient adressés dans les institutions et qui étaient les auteurs des demandes restées sans réponse.

L'autre chose, c'est que nous serions disposés à mener une étude à ce sujet et, en groupes, à retourner pour le définir et tenter de le quantifier, encore par l'entremise de notre partenaire à l'ABC. Mais cela nous prendra un certain temps.

Enfin, si je puis parler au nom de mon institution et des autres, nous ne croyons pas qu'un crime soit un avantage concurrentiel. Nous collaborons bel et bien, et nous voulons réellement y mettre un frein. Nous travaillons avec nos partenaires de l'industrie, comme vous avez entendu mes pairs le formuler, sur les meilleures stratégies à adopter, par la sensibilisation ou d'autres mesures, pour informer le public ainsi que pour arrêter les conséquences du vol d'identité, sans compter le vol d'identité proprement dit.

M. Mathieu Ravignat: Vous êtes au moins conscient du fait que les universitaires tentent de communiquer avec vos institutions afin d'obtenir des renseignements pour étudier la question.

M. Ed Rosenberg: Depuis cette semaine, nous le sommes.

Encore une fois, je suis responsable à l'égard des actes frauduleux commis à l'intérieur de la banque en tant que telle. Aucun membre de mon personnel ni personne à l'intérieur de ma filière hiérarchique n'a jamais été abordé; nous ne savons donc pas vraiment à qui cette demande a été adressée en réalité.

M. Mathieu Ravignat: C'est bizarre.

Nous avons entendu le témoignage de personnes et de bandes des Premières Nations qui ont indiqué que le problème du vol d'identité est lié à un manque d'accès à l'information par de nombreux membres des Premières Nations. Certaines bandes se sont plaintes du fait que les banques profitaient de cette situation particulière, surtout du manque d'information du bureau de crédit, pour créer un crédit à la consommation qui va bien au-delà des limites acceptables. Il y a de nombreux exemples de personnes des Premières Nations à qui on facture des taux d'intérêt de 300 % plus élevés qu'aux non-Autochtones.

Essayez-vous de vous attaquer à certains des problèmes inhérents au fait de traiter avec des Premières Nations? Vos institutions ont-elles mis en place un processus de consultation pour faire affaire avec une population qui est beaucoup plus vulnérable au vol d'identité que les autres?

● (1140)

Le président: Monsieur Milkman, souhaitez-vous répondre?

M. Paul Milkman: Oui. Je ne suis pas certain que je pourrai donner une réponse précise. En tant qu'institutions de commerce de détail, les stratégies de nos succursales, surtout dans les régions principalement peuplées par des Premières Nations, offrent divers types de formations et de documents pour tenter d'aider à régler le problème. Mais je pense que la plupart d'entre nous dirions probablement que ce n'est pas tellement notre secteur d'activité, et nous souhaiterions vous présenter certaines informations sur ce que nous ferions différemment.

M. Mathieu Ravignat: Nous vous en serions certainement reconnaissants. Vous pourriez peut-être discuter avec vos diverses organisations du fait qu'il s'agit bel et bien d'un problème. J'ai deux Premières Nations dans ma circonscription, et bon nombre de mes collègues en ont également. Les Premières Nations se font escroquer, et les taux de vol d'identité sont plus élevés dans ces collectivités. Nous devons intervenir.

J'aimerais revenir à ma question précédente, mais peut-être du point de vue d'un consommateur.

Il y a une tension entre la tenue de renseignements financiers, le fait que vous devez être concurrentiels, vos produits à l'interne et la sensibilisation du public de même que le lien avec le vol d'identité dans ce contexte. Comment fournissez-vous des outils aux consommateurs pour vous assurer qu'ils ont accès à ce dont ils ont besoin pour empêcher leur identité d'être volée? Je ne parle pas de mesures postérieures au vol d'identité; je parle de prévention. Ce n'est pas nécessairement au gouvernement qu'il incombe de le faire.

M. Philip Fisher: Je serais heureux d'aborder cette question.

Tout d'abord, la CIBC ne verrait pas la sécurité et l'intégrité des renseignements de ses clients comme un avantage concurrentiel ou une chose à propos de laquelle elle voudrait être en concurrence avec quiconque. Nous considérerions cela comme une attente de la part du consommateur, que ses renseignements soient protégés.

Je pense que c'est important, du point de vue des outils de sensibilisation. Nous tenons le client au courant de ce qui se passe avec son compte. Par l'intermédiaire de son service bancaire en ligne, la CIBC émet diverses alertes de transaction. Vous pouvez y aller pour voir quand vos renseignements personnels changent, quand votre NIP change, quand votre mot de passe change ou quand toute transaction importante est effectuée. Nous offrons même la surveillance gratuite du bureau de crédit. Nous le faisons parce que nous pensons qu'il est important pour le client de savoir ce qui se passe relativement à son compte et de le savoir en temps réel. Les clients qui s'inscrivent à ces services reçoivent un courriel ou un message texte leur disant ce qui se passe avec leur compte, en temps réel, afin qu'ils puissent intervenir et poser des questions à l'organisation.

Le président: Nous allons devoir en rester là, monsieur Fisher. Merci beaucoup.

Votre temps est écoulé, monsieur Ravignat.

Pour le Parti conservateur, nous avons David Anderson. Bienvenue au comité, monsieur Anderson.

M. David Anderson (Cypress Hills—Grasslands, PCC): Je vous remercie, monsieur le président. C'est un plaisir pour moi d'être ici aujourd'hui.

Quand vous parlez de mesures comme le renvoi de courriels et de messages texte et ce genre de choses, l'accès est-il obtenu au niveau du mot de passe? Est-il obtenu à l'échec de l'ouverture de session d'un site: une personne pourrait y accéder grâce à cet échec? Est-il obtenu par le truchement de sites Web factices? Depuis quelque temps, une de vos banques m'envoie quelque chose qui ne provient manifestement pas de vous, et je me demande, quand on rencontre ce genre de problèmes, où se situe habituellement le point d'accès.

● (1145)

M. Philip Fisher: Il y en a en fait plusieurs. Vous en avez nommé quelques-uns. L'essentiel, c'est que nous observons un nombre considérable de courriels de hameçonnage; nous voyons des logiciels malveillants dans l'ordinateur des clients — c'en est un que je soulignerais comme étant extrêmement problématique — et nous voyons des clients fournir leurs renseignements à des tiers, puis constater que ces tiers les divulguent. Mais je pense que l'accès par chacun de ces points fluctue.

Si vous me posez des questions au sujet du hameçonnage, je vous dirais que le nombre d'incidents de hameçonnage a augmenté au fil des ans, mais que le nombre de clients qui en sont victimes a diminué au fil des ans. Quand j'ai commencé à faire ce travail, j'ai effectué un calcul approximatif, selon lequel, pour chaque courriel hameçon qui était diffusé, je constatais que 40 clients avaient fourni leurs renseignements. Maintenant, je constate que, en moyenne, de un à un demi-client fournit ses renseignements à ces sources.

Vous avez montré votre appareil mobile. C'est un des problèmes. Les gens qui ont un grand écran peuvent voir les aspects visuels qui indiquent que quelque chose ne va pas à cet égard, mais, si on réduit l'affichage à celui d'un appareil mobile, il devient beaucoup plus difficile de repérer les indices qui pourraient vous dire que quelque chose ne va pas.

M. David Anderson: Je ne m'y connais pas beaucoup à ce sujet, mais, souvent, on retourne à l'adresse de courriel. C'est vraiment la seule chose qui, selon moi, vend la mèche, parce qu'il y a des sites Web dont la présentation est assez attrayante.

Je veux vous demander quel pourcentage des activités criminelles sont liées à ce qu'on pourrait appeler des tentatives insignifiantes d'obtenir des renseignements et quel pourcentage serait beaucoup plus imputable au crime organisé. Je pense que Mme Frook a parlé du fait que cette technologie est évolutive, qu'elle évolue rapidement, qu'elle est changeante et qu'elle est sophistiquée. Est-ce de plus en plus l'oeuvre du crime organisé ou encore de personnes qui font du piratage de chez elles et qui sont plutôt intelligentes, puisqu'elles peuvent déjouer ces systèmes?

M. Philip Fisher: Il est certain que les actes frauduleux liés aux cartes, comme le fait de copier des cartes de débit et de crédit, sont le domaine où on a tendance à observer la plus grande implication de groupes du crime organisé. Mais, lorsqu'il est question de hameçonnage et de logiciels malveillants, les obstacles à l'accès pour les fraudeurs sont considérablement réduits. Vous pouvez aller sur Internet et acheter une trousse qui vous aidera à hameçonner une banque. Vous avez besoin de très peu de capacités techniques. Vous achetez cette trousse; elle fait tout le travail pour vous, et elle transmet les renseignements.

Vous allez commencer à observer un plus grand nombre de personnes qui comparaissent relativement à certains de ces types d'actes frauduleux, puisque c'est le genre de choses qu'on fait par soi-même comparativement aux types d'actes frauduleux liés aux cartes de débit et de crédit commis par le crime organisé.

M. David Anderson: D'accord.

Mes institutions financières m'envoient régulièrement leurs ententes en ligne. Elles n'arrêtent pas de changer. Elles sont constamment modifiées. De toute manière, elles sont pratiquement indéchiffrables pour la personne moyenne, mais une des choses que la plupart d'entre elles semblent avoir en commun, c'est qu'elles semblent réduire la responsabilité de l'institution chaque fois que j'en reçois une, et augmenter ma responsabilité.

Entendez-vous dire par le public qu'il est frustré par ce genre de choses? Lorsque je les reçois, j'ai l'impression qu'il pourrait y avoir eu un certain changement technologique, mais c'est habituellement parce qu'on dirait que l'institution financière tente de se décharger d'une responsabilité plutôt que d'améliorer ma protection.

Quelqu'un a-t-il un commentaire à formuler?

M. Philip Fisher: Je peux poursuivre, si vous voulez.

Il est certain qu'il est quelque peu intimidant pour les consommateurs d'étudier certaines de ces ententes d'accès électronique. Par contre, du point de vue d'une banque, nous tentons de comprendre le fait que nos clients ne sont pas experts en matière de technologie ni en matière de sécurité de l'information; ainsi, nous tentons de faire en sorte que leurs attentes restent assez peu élevées. Nous voulons que vous vous dotiez d'un antivirus, et nous voulons que vous tentiez de protéger votre ordinateur, mais nous comprenons que c'est difficile à faire pour certains clients.

Nous examinons ces cas au cas par cas. En en étudiant un, nous nous demandons si nous ne commettons pas une erreur au profit du client: lui accordons-nous le bénéfice du doute?

Le président: Monsieur Fisher, je vais devoir vous interrompre.

Monsieur Anderson, vous savez que la cloche sonne.

Avec le consentement unanime du comité, nous pourrions prolonger cette séance de 15 minutes environ. Il y a des cloches aux demi-heures, et nous sommes dans le même immeuble.

Le comité est-il disposé à poursuivre pour 15 minutes?

Des voix: D'accord.

Le président: Bien, nous avons une entente.

Poursuivez, monsieur Anderson. Il vous reste environ deux minutes de votre tour de sept minutes.

M. David Anderson: Merci, monsieur le président.

Ma question concerne les petites choses dans ces ententes. Dans quelle mesure est-il réaliste de demander aux gens de changer leur mot de passe tous les 90 jours quand ils utilisent des mots de passe à une douzaine d'endroits différents? Vous n'avez pas le droit d'utiliser le même; ainsi, on s'attend à ce que vous teniez des comptes différents et que vous changiez de mot de passe régulièrement. Je pense simplement que, pour certaines personnes, ça va, mais, pour de nombreuses autres, c'est une vraie source de frustration.

Comment peut-on composer avec cette frustration?

M. Philip Fisher: Il est certain que, du point de vue de la CIBC, nous n'exigeons pas que vous changiez votre mot de passe bancaire en ligne tous les 30 jours. Nous comprenons qu'il est difficile pour les clients de se souvenir de leur mot de passe. Même à l'intérieur de notre propre site, on a parfois besoin de plusieurs mots de passe ou de questions de vérification personnelles.

Du point de vue de l'évolution des services bancaires en ligne, la CIBC est en train d'adopter un système d'authentification à deux facteurs qui sera lancé le mois prochain. Nous allons retirer certaines des questions de vérification personnelles, et nous allons commencer à envoyer aux clients des messages textes contenant des codes à usage unique qu'ils utiliseront lorsqu'ils veulent effectuer une transaction à risque élevé et lorsqu'ils en ont réellement besoin, afin que la sécurité soit placée là où elle doit l'être, au moment où le client en a besoin. Nous allons tenter de faire en sorte qu'ils n'aient pas besoin de se souvenir de toutes ces choses.

● (1150)

M. David Anderson: J'ai probablement le temps de ne poser qu'une question de plus, mais je veux savoir quelle est la différence entre la protection américaine et la protection canadienne. Il me semble que certaines technologies semblent accuser du retard aux États-Unis. Je pense que nous sommes à l'avant-garde dans un certain nombre de domaines à cet égard. Ici, on obtient les cartes à bande magnétique. Là-bas, on obtient un échec de tentative de transfert d'argent par voie électronique. Comment est-ce que cela contribue à ce genre de vol d'identité et de fraude ou comment est-ce que cela permet de les prévenir?

M. Paul Milkman: Bien entendu, TD a une présence très importante aux États-Unis et est la plus importante banque à réseau étrangère exploitée aux États-Unis. Ce que nous observerions, c'est qu'il y a des variations sur le plan des mesures de protection entre les deux pays. Nous dirions que la puce et le NIP, en particulier, présentent un énorme avantage pour les consommateurs canadiens. Honnêtement, ayant vu des données des deux côtés de la frontière, nous dirions que nous avons observé des techniques comme l'écrémage aux guichets automatiques qui ont littéralement migré au sud de la frontière en raison du contrôle supérieur de l'environnement canadien. Nous dirions qu'il y a d'autres domaines où, selon moi, les grandes institutions des États-Unis et du Canada travaillent très dur pour accélérer leurs efforts. L'analytique des données sur les transactions, c'est-à-dire la collecte de renseignements sur ce à quoi ressemble une transaction normale dans nos banques, est une chose sur laquelle les deux pays travaillent très dur. On pourrait dire qu'il y a un ensemble de problèmes communs sur lesquels nous travaillons tous. Actuellement, le Canada présente certainement certains avantages par rapport aux États-Unis.

L'autre aspect qui est différent, je crois, au Canada, c'est que les banques et certains autres intervenants clés de l'industrie, comme les entreprises de télécommunications, travaillent en plus étroite collaboration avec les responsables de la sécurité publique. La possibilité d'un changement législatif, voire même d'un changement d'interprétation d'une loi existante au Canada permettra fort probablement au Canada de dépasser les États-Unis pour ce qui est de faire des progrès à l'échelle nationale. Ici, le partenariat public-privé est un peu plus accessible. Aux États-Unis, on observe des signes selon lesquels les Américains continueront probablement d'accuser du retard en ce qui a trait à l'adoption de lois vraiment avant-gardistes sur la protection des renseignements personnels et sur la sécurité en soi.

Le président: Monsieur Milkman, je dois vous interrompre là.

Merci, monsieur Anderson.

Pour le Parti libéral, M. Scott Andrews, pour sept minutes.

Nous aurons probablement du temps à vous accorder pour que vous procédiez à votre série de questions. Je suis heureux parce que les trois partis auront eu l'occasion d'en poser. Ensuite, nous allons libérer nos témoins en les remerciant, ajourner la séance et aller voter. Je vais demander aux membres du comité de revenir pour 10 ou 15 minutes. Il faut que nous discutions d'affaires et de témoins à venir pour mardi prochain.

Sur ce, monsieur Andrews, pour sept minutes.

M. Scott Andrews (Avalon, Lib.): Merci beaucoup, monsieur le président.

Monsieur Fisher et monsieur Stark, je pense que vous avez tous deux mentionné que la définition du terme « vol d'identité » n'est pas toujours la même. Voulez-vous donner plus de détails à ce sujet, puisque nous étudions le vol d'identité? Quelle est la définition que nous devrions approfondir?

M. Jay Stark: Un des exemples clés serait l'écrémage des cartes de crédit et des cartes de débit. Certaines personnes considéreront les cartes de débit et les cartes de crédit comme englobant le vol d'identité, dans ce cas. Bien des banques ne tiennent pas compte de cela. Nous étudions davantage les choses lorsque des identifiants sont volés, ou il pourrait s'agir de documents ou de données du bureau de crédit, et une demande est présentée à une banque au nom d'une autre partie. Ce serait du vol d'identité. Mais, en réalité, les problèmes importants que nous avons sont liés aux zones grises.

Dans ma déclaration préliminaire, je voulais présenter le crime financier dans son ensemble; ensuite, nous aurions fractionné du mieux que nous l'aurions pu les aspects sur lesquels nous nous entendions relativement au vol d'identité, puis aurions montré les zones grises afin que le comité puisse les étudier et se forger sa propre opinion.

M. Philip Fisher: Du point de vue de la CIBC, nous avons tendance à surveiller la fraude à un niveau bien inférieur, plus détaillé. Une partie de cette surveillance est opérationnelle et organisationnelle, c'est-à-dire, disons, qu'une équipe est responsable du vol d'identité. Nous avons une équipe consacrée au vol d'identité. Les membres de cette équipe ont un ensemble défini de fonctions et de responsabilités à l'égard de certains types de fraude, qui pourrait être différent selon la façon dont une autre organisation les diviserait. Lorsque nous parlons de faire remonter l'information jusqu'à l'échelon du vol d'identité, le problème que nous avons est de nous assurer que nous mettons les pommes avec les pommes et que l'on place les renseignements de même type dans la même catégorie. Ainsi, ce que nous fournissons a manifestement de l'importance, n'est-ce pas?

● (1155)

M. Scott Andrews: Pour ma part, depuis les quelques jours où je siège au comité, je me suis efforcé de tenter de compartimenter les personnes qui sont en fait des gens. Je pense que personne n'a parlé du vol d'identité « synthétique ». Cela provient de notre dernière séance de groupe. Il y en a des activités qui touchent de vraies personnes, et d'autres qui sont du vol d'identité « synthétique ». Quelle est l'ampleur du vol d'identité « synthétique » à la banque?

M. Ed Rosenberg: Laissez-moi répondre à cette question.

Encore une fois, je pense que ce que Philip tentait d'expliquer, c'est que nous voyons la fraude très différemment. Ces deux formes, qu'il s'agisse d'une personne fictive ou d'une vraie personne, se manifesteront dans le vol d'identité, si vous voulez, ou la fraude dans notre pays. Toutefois, nous les considérerions comme des risques importants.

L'identité « synthétique » est une préoccupation importante pour nous. L'un des problèmes que nous avons est de nous assurer que, lorsque nous authentifions un client et validons l'activité transactionnelle qu'il effectue, nous disposons d'un certain mécanisme qui nous permet de faire une comparaison, par exemple, pour dire qu'il s'agit de M. Andrews et que ces transactions sont celles de M. Andrews et que, par conséquent, nous allons accepter ou effectuer les transactions pour lui.

C'est difficile pour nous. L'identité « synthétique » est une préoccupation importante parce que nous n'avons aucune emprise sur l'établissement de l'identité, sur la production de cette pièce d'identité, mais nous faisons face à la manifestation lorsqu'elle nous est présentée pour effectuer ces transactions.

Ce sont deux sujets très importants pour nous. Pour les quantifier, il faudrait étudier de façon plus approfondie nos systèmes respectifs afin d'en tirer le nombre.

M. Scott Andrews: Cela m'amène à ma prochaine question parce que, monsieur Fisher, vous avez mentionné la surveillance gratuite du crédit. Des représentants d'agences d'évaluation du crédit sont venus ici. Je pense qu'ils font partie du personnel de première ligne, mais ils vont dire: « non, nous sommes un genre de personnel de première ligne, mais les banques sont en première ligne ». Qui est en première ligne lorsqu'il s'agit de sonner l'alarme?

Concernant la surveillance gratuite du crédit que vous avez mentionnée, monsieur Fisher, je veux seulement approfondir un peu le rôle des agences d'évaluation du crédit et la relation avec l'industrie bancaire.

M. Philip Fisher: En ce qui concerne la surveillance gratuite du bureau de crédit, nous entretenons une relation avec le bureau de crédit. Nos clients peuvent se rendre sur notre site et s'inscrire à ce service. Ensuite, si le bureau de crédit reçoit une demande de renseignements sur le compte du client, ce qui arrive, c'est qu'il nous transmet l'information, puis nous finissons par l'envoyer au client pour qu'il fasse son enquête.

Nous disons au client quel commerçant a demandé des renseignements sur son dossier au bureau de crédit, de quel genre de demande il s'agissait et quand elle a été présentée. Il arrive même qu'on ait accès aux coordonnées du commerçant qui a présenté la demande de renseignements.

Dans ce cas précis, nous protégeons le bureau de crédit.

M. Jay Stark: En fait, nous avons établi une relation avec les bureaux de crédit, et plus particulièrement avec Equifax, où nous filtrons tous les crédits à l'aide de bases de données analytiques et négatives. Je pense donc qu'il s'agit d'un effort déployé conjointement par les bureaux de crédit et les banques.

M. Scott Andrews: L'autre chose que vous avez mentionnée concernait la fraude par chèque, monsieur Stark. Pouvez-vous comparer de façon un peu plus détaillée la fraude par chèque et le vol d'identité? Sont-ils distincts?

M. Jay Stark: Je pense que, là où M. Rosenberg voulait en venir, c'est que nous devons y consacrer un peu plus de temps et suivre le cycle en entier.

Nous observons certaines manifestations du vol d'identité dans le domaine des chèques. Une personne pourrait s'emparer d'un compte... une prise de contrôle du compte. Ce qui me préoccupe davantage, c'est l'endroit où vont les fonds et donc l'endroit où les fraudeurs vont. Nous suivons ces fraudeurs et les désignons. Nous voyons un certain nombre de situations où des gens se présentent avec de fausses pièces d'identité pour constituer une société, par exemple, et être le propriétaire bénéficiaire, où ils en seront les administrateurs. Ces cas sont un peu plus problématiques parce que, à partir de là, ils vont blanchir des fonds.

Nous passons beaucoup de temps à étudier ce problème. Nous passons également un certain temps à observer la prise de contrôle du compte d'une personne en particulier.

La fraude par chèque est assez prévalente, qu'il s'agisse du vol d'une pièce d'identité ou pas, ou que ce soit un simple acte frauduleux. Nous appelons cela une fraude de première partie.

Le président: Merci beaucoup, Scott. J'ai bien peur que ce soit tout le temps que je puisse vous accorder.

Je pense qu'il nous reste assez de temps pour procéder à nos votes, mais j'aimerais tout d'abord que vous précisiez un élément de votre témoignage, madame Frook.

On a de plus en plus l'impression que le public a le droit de savoir si ses renseignements personnels ont été compromis. On parle d'une obligation de notification prévue dans une loi en voie d'être adoptée. Dans le cadre de votre témoignage, vous avez dit que, selon votre politique, vous devez aviser la personne, pas la commissaire à la protection de la vie privée ni le bureau de crédit, si son identité a été compromise ou si un acte frauduleux est commis dans son compte.

À ce que nous sachions, ce n'est pas le cas. Ma carte de crédit peut être compromise, et vous allez corriger la situation et vous allez corriger et rétablir la situation, mais je ne saurai jamais que cela s'est produit.

La politique de votre banque vous oblige-t-elle à dire à toutes les victimes de vol d'identité que leurs renseignements personnels ont été compromis?

● (1200)

Mme Jennifer Frook: Dans le cas précis que vous avez mentionné, en ce qui concerne une fraude par carte de crédit, à la Banque Scotia, lorsque nous apprenons qu'un certain nombre de nos clients ont été victimes d'une compromission, nous communiquons avec nos clients. Nous leur expliquons que nous croyons que leur carte de crédit a été compromise et que nous allons prendre des mesures proactives pour les protéger contre les actes frauduleux qui pourraient être commis dans leur compte.

Le président: Et s'il ne s'agit que d'une seule personne? Vous avez dit lorsqu'il s'agit d'un groupe. Manifestement, si c'était un problème important, comme lorsque la CIBC a eu tous ses ennuis, le public était au courant, mais que feriez-vous s'il s'agissait d'une personne?

Mme Jennifer Frook: Même dans les cas où il ne s'agit que d'une personne, encore une fois, je réponds précisément à vos commentaires concernant la fraude par carte de débit et de crédit, à la Banque Scotia, nous ne nous contenterions jamais de simplement bloquer votre accès au crédit. Nous tenterions de vous aviser. Nous aimons beaucoup certaines des technologies dont nous disposons, qui nous permettent de vous joindre par voie électronique. Vous n'avez pas à attendre ce message téléphonique à la maison; nous pouvons vous alerter immédiatement.

Le président: Cela ne répond pas vraiment à la question...

Mme Jennifer Frook: Je suis désolée. Je m'excuse...

Le président: Là où je veux en venir, la question que j'essaie de vous poser, c'est la suivante: du point de vue des cinq grandes banques à charte, seriez-vous en faveur de l'obligation de notification qui est envisagée dans la loi qui sera bientôt adoptée? Cela signifie que vous seriez tenues d'informer la victime du fait que son identité personnelle a été compromise. Est-ce votre pratique, actuellement? Appuieriez-vous sa codification et seriez-vous d'accord pour qu'elle soit codifiée et prévue dans une loi?

M. Paul Milkman: À TD, la pratique en vigueur veut que nous avisions toutes les personnes dont l'identité a été compromise ou lorsque nous soupçonnons que leur identité a été compromise. Dans toutes les situations matérielles ou les situations systémiques importantes, nous aviserions également les organismes de réglementation, la commissaire à la protection de la vie privée, etc. mais, au cas par cas; pour répondre à votre question précise, notre politique actuelle exige que nous le fassions.

Mme Jennifer Frook: On ferait de même à la Banque Scotia.

Le président: Je pense que nous sommes pas mal à court de temps, mesdames et messieurs. Nous allons suspendre la séance. Si cela les intéresse, peut-être que d'autres personnes aimeraient répondre à la même question. Il s'agit d'une question de premier ordre pour bien des Canadiens, et c'est une chose contre laquelle nous luttons, au moyen d'une loi.

Monsieur Rosenberg.

M. Ed Rosenberg: Je crois que, en général, nous sommes favorables au modèle et à la loi proposée devant la Chambre. C'est la première déclaration.

La deuxième, concernant le cas par cas, c'est que la plupart de nos systèmes ne sont pas conçus pour repérer la fraude à l'échelon individuel. Je pense que M. Fisher a mentionné que nous nous fions à nos clients pour qu'ils examinent leurs propres transactions. De fait, ils deviennent la première ligne de défense pour nous. Cela devient ensuite une relation personnelle avec le client et, grâce à ce dialogue, s'il est victime d'un vol d'identité, nous l'aidons à prendre des mesures pour le protéger, et la banque a l'obligation de le faire.

Le président: Monsieur Stark.

M. Jay Stark: Je répéterais le commentaire du représentant de TD.

Nous avisons les personnes, et nous aviserions la commissaire à la protection de la vie privée s'il s'agissait d'une atteinte pertinente ou importante. Nous avons un comité mixte de la conformité et de la fraude et un certain nombre d'autres parties qui étudieraient la situation et s'assureraient que les paramètres appropriés ont été établis pour garantir que la commissaire à la protection de la vie privée sera avisée.

Le président: Monsieur Fisher.

M. Philip Fisher: Le point de vue de la CIBC est le même que celui des autres témoins.

Le président: D'accord, c'est très utile.

Merci beaucoup, mesdames et messieurs. Nous allons suspendre la séance. Nous allons remercier nos témoins et les excuser. Nous nous réunirons ici tout de suite après le vote pour une séance de planification d'une dizaine de minutes, à huis clos.

- _____ (Pause) _____
-

[*La séance se poursuit à huis clos.*]