Consumer Measures Committee

Comité des mesures en matière de consommation

Travailler ensemble pour prévenir le vol d'identité

Document de discussion

Travailler ensemble pour prévenir le vol d'identité

Document de discussion aux fins de consultation publique
6 juillet 2005

Introduction

Les nouvelles technologies de l'information ont révolutionné les pratiques commerciales des entreprises canadiennes en les rendant plus efficientes et plus compétitives. En même temps, toutefois, la collecte et l'entreposage électroniques de renseignements personnels ont multiplié les risques liés à l'obtention et à l'utilisation frauduleuses de ces renseignements en vue de commettre une fraude ou un autre type de crime. C'est ce qu'on appelle le « vol d'identité ».

Il est difficile d'évaluer l'ampleur réelle de ce problème puisque les personnes touchées font part de leurs plaintes à différents organismes, y compris les bureaux de crédit[1], les banques, les sociétés de cartes de crédit, les services de police ou les ministères. De plus, un grand nombre de victimes ne signalent pas qu'il y a eu vol d'identité. Néanmoins, les sondages auprès des ménages montrent que le problème est important. En février 2003, Ipsos Reid indiquait que 9 p. 100 des Canadiens, soit environ 2 700 000 personnes, avaient, à un moment ou à un autre, été victimes d'un vol d'identité[2]. Les victimes essuient des pertes financières; leur réputation est entachée, et elles subissent un stress émotionnel. De plus, elles doivent, souvent avec difficulté, rétablir leur cote de crédit[3].

Le présent document de discussion explore un certain nombre d'options visant à modifier les lois fédérales, provinciales et territoriales dans le but de compliquer la tâche des voleurs d'identité et de permettre aux victimes de surmonter plus facilement cette expérience. Les options politiques liées au *Code criminel* sont examinées par le ministère de la Justice dans le cadre d'un processus distinct et elles ne sont pas incluses dans le présent document.

Le document est divisé en quatre sections. Dans la première, on fournit un aperçu du problème que représente le vol d'identité, y compris la définition des termes et les exemples spécifiques des préjudices qu'entraîne ce type de fraude. Dans la section suivante, on explique pourquoi le vol d'identité est en croissance et on nomme les groupes qui pourraient contribuer à la solution. La troisième section brosse un tableau du cadre législatif actuel au Canada et aux États-Unis. Enfin, dans la quatrième section, on propose des options de réforme législative visant à lutter contre le phénomène, en exposant le pour et le contre de chaque option, et l'on soumet certaines questions à l'examen du lecteur.

Demande de commentaires

Le Comité des mesures en matière de consommation (CMC) est formé de représentants des gouvernements fédéral, provinciaux et territoriaux qui travaillent de concert à éliminer les obstacles au commerce interprovincial et inter-territorial et à améliorer le marché à l'intention des consommateurs canadiens. Le CMC a organisé des consultations publiques sur les moyens de lutter contre le vol d'identité dans le but d'obtenir l'opinion des intervenants et des membres du public quant aux répercussions politiques et pratiques de ces mesures. Le CMC pourra ensuite revoir les propositions et les étoffer en fonction des commentaires des intervenants. Il organisera ensuite une autre série de consultations sur des propositions spécifiques, présentées en langage quasi-juridique, en indiquant quelles lois pourraient être touchées.

L'objectif du présent document est de faciliter la participation du public au processus de réforme en établissant le contexte du problème et en proposant une première analyse des diverses options de réforme.

Afin d'aider le CMC à examiner ces propositions, nous vous prions de structurer vos commentaires en vous basant sur le document de consultation. Plus précisément, nous vous demandons de fournir des réponses aux questions individuelles, et d'y ajouter les commentaires que vous souhaitez apporter. En outre, nous vous prions de mettre l'accent sur les réalisations auxquelles on peut raisonnablement s'attendre au cours des 10 prochaines années et de fournir plus de renseignements et de preuves à l'appui, dans la mesure du possible.

Nous demandons à toutes les parties de prendre toutes les mesures possibles pour aider le CMC à atteindre le défi de taille qui consiste à élaborer des recommandations en vue de préparer le meilleur cadre pour lutter contre le vol d'identité – indépendamment des coûts et des avantages à court terme pour les différents acteurs de l'industrie ou les groupes de consommateurs.

Il serait grandement apprécié que vous soumettiez vos commentaires de façon électronique. Pour ce faire, veuillez visiter notre site Web (www.cmcweb.ca/volidentite) et télécharger le Livret de consultation sur le vol d'identité. Une fois vos réponses incorporées, veuillez en faire l'envoi par courriel au:

Courriel: info@cmcweb.ca

Si vous préférez soumettre ce livret en copie papier, veuillez le faire parvenir à l'adresse suivante, accompagné de votre nom et de vos coordonnées:

Télécopieur : (613) 952-6927
Poste : Comité des mesures en matière de consommation
Bureau de la consommation
Industrie Canada
235, rue Queen
Ottawa (ON) K1A 0H5

Si vous désirez soumettre vos commentaires sur le *Document de discussion* et ses options, il n'est pas essentiel d'utiliser le *Livret de consultation*. Vous pouvez présenter vos commentaires sous forme de lettre ou courriel. Il est aussi possible de répondre uniquement aux questions de votre choix (vous n'avez pas à répondre à toutes les questions).

Tous les documents ou commentaires transmis par différents organismes sont susceptibles d'être utilisés ou publiés par le CMC ou par un autre organisme gouvernemental dans le but de soutenir l'évaluation et l'examen des options proposées, décrites ci-dessous. Il se pourrait donc que des documents, des commentaires ou des résumés soumis par un organisme soient communiqués aux autres parties intéressées, pendant ou après la période des commentaires publics.

On considérera qu'une personne qui fournit des documents ou fait part de commentaires en indiquant qu'elle fait partie d'un organisme le fera au nom de cet organisme.

Les documents et commentaires fournis par une personne qui n'indique pas qu'elle fait partie d'un organisme pourront être utilisés et communiqués dans le but d'aider de CMC ou d'autres organismes gouvernementaux à revoir les options proposées et les évaluer. Quoi qu'il en soit, le CMC et les autres organismes gouvernementaux ne divulgueront aucun renseignement de nature personnelle, par exemple le nom de la personne ou ses coordonnées, sauf si la loi l'exige.

Définir le vol d’identité

La définition de « vol d’identité » suscite encore beaucoup de confusion, surtout quand on l’envisage sous l’angle de l’appropriation de renseignements personnels par des tiers. En vertu des lois canadiennes, le vol d’information est impossible, puisque la personne concernée par ces informations les possède toujours. Autrement dit, il n’y a pas eu vol, puisque la personne possède encore ces informations; tout ce qui a été perdu, c’est leur caractère confidentiel[4]. Beaucoup considèrent qu’il s’agit d'une lacune du *Code criminel*. D’autres projets sont en cours, au gouvernement fédéral, afin de proposer des modifications visant à mieux lutter contre cette criminalité. Mais en ne comptant que sur les dispositions pour freiner les « voleurs », on laisse de côté des aspects plus fondamentaux du problème qui font que la technologie et les pratiques commerciales dans leur ensemble peuvent, sans le vouloir, faciliter la fraude.

Aux fins du présent document, on définit le vol d’identité comme le fait, pour une personne, d’utiliser les renseignements personnels qui concernent une autre personne, à l’insu de celle-ci et sans son consentement, pour commettre un crime, par exemple une fraude, un vol ou la contrefaçon. Cette définition nous permet d'aborder le problème dans son ensemble – depuis la collecte des informations jusqu’à la diffusion des informations, leur utilisation frauduleuse, et les mesures correctives – et de cerner des moyens d’atténuer le préjudice subi par le consommateur.

En vertu de la *Loi sur la protection des renseignements personnels et les documents électroniques* (LPRPDE), un renseignement personnel s’entend de : « Tout renseignement concernant un individu identifiable, à l’exclusion du nom et du titre d’un employé d’une organisation et des adresse et numéro de téléphone de son lieu de travail ». Au Québec, la *Loi sur la protection des renseignements personnels dans le secteur privé* définit un renseignement personnel comme étant « tout renseignement qui concerne une personne physique et permet de l'identifier ». Cela comprend notamment le nom d’une personne, son adresse, son âge, son sexe, ses numéros d’identification, ses numéros de cartes de crédit, son revenu, son emploi, son actif et son passif, ses sources de revenu, ses relevés de paiement, ses références personnelles et ses dossiers de santé. En général, cela *ne comprend pas* ses coordonnées au travail, mais cela peut comprendre l’adresse électronique au travail.

Les victimes de vol d'identité subissent divers préjudices : on utilise leurs renseignements personnels pour ouvrir un nouveau compte de carte de crédit (36 %), faire des paiements frauduleux ou commettre une fraude à l'assurance (24 %), obtenir des prestations du gouvernement (24 %), ouvrir un compte auprès des services publics ou des compagnies de téléphone (23 %) ou obtenir un prêt en usurpant le nom de la victime (22 %)[5]. On peut aussi utiliser ces renseignements personnels pour commettre un vol ou produire de faux documents. Par exemple, un voleur d'identité qui détient le numéro de carte de débit et le numéro d’identification personnel (NIP) d’une autre personne peut utiliser ces informations pour vider le compte en banque de la victime (vol). Il peut aussi utiliser les informations qui concernent cette autre personne pour falsifier une demande de passeport ou un chèque (contrefaçon). Il peut

ensuite déposer ce faux chèque dans le compte de sa victime, puis effectuer un retrait – et ce sera à la victime de combler le manque à gagner.

Il ne faut surtout pas perdre de vue le fait que le vol d'identité ne se fait pas toujours à des fins personnelles. Un rapport présenté au Solliciteur général du Canada et au Procureur général des États-Unis indique que le vol d'identité se fait couramment dans le but de faciliter d'autres activités criminelles, par exemple la criminalité organisée ou le terrorisme[6]. En réduisant le nombre de vols d'identité, on favorise aussi la réduction des préjudices sociaux plus généraux, comme les menaces à la sécurité nationale.

Comprendre le problème

Les vols d'identité sont de plus en plus fréquents. Selon des sondages réalisés au Canada et aux États-Unis, près de 3 % des Canadiens et des Américains ont été victimes d'un vol d'identité, uniquement en 2003[7].

Les fraudes et les vols ne sont pas un phénomène nouveau. Ce qui est nouveau, c'est l'échelle à laquelle ces crimes sont commis. Les criminels peuvent utiliser des bases de données électroniques pour s'approprier frauduleusement des renseignements personnels et les utiliser de manière illégale pour obtenir des prestations ou du crédit à la consommation. L'agence d'évaluation du crédit commercial et à la consommation TransUnion LLC signale que le nombre de vols d'identité est passé de 4 000 en 1999 à plus de 24 000 en 2002 (une augmentation de 500 %). [8]

Le comportement des consommateurs peut aussi présenter un risque de vol d'identité, par exemple lorsqu'une personne ne protège pas son NIP, lorsqu'elle fournit plus d'informations qu'il n'est nécessaire ou qu'elle fait des paiements en ligne sur des sites Web qui ne sont pas protégés.

Les pratiques commerciales contribuent elles aussi au problème. Selon Judith Collins, qui enseigne à l'Université Michigan State, jusqu'à 70 % des vols d'identité peuvent être liés à des fuites *de l'intérieur* d'un organisme. C'est le cas par exemple lorsqu'un employé accepte un pot-de-vin en échange d'informations ou qu'il subtilise des informations des clients pour le compte du crime organisé[9]. Les employés ou voleurs peuvent également voler de l'équipement pour sa valeur de revente, et non pour l'information qu'il contient. La société d'assurance-vie Co-operators de la Saskatchewan a été victime de ce type d'infraction en janvier 2003 : un des employés de son entreprise de gestion de données s'est enfui avec un disque dur contenant les renseignements personnels de quelque 180 000 clients.[10]

Récemment, au Canada, des infractions visant des données ont fait craindre que les informations volées ne servent à commettre des vols d'identité. En février 2004, un bris de sécurité de la société Equifax a visé le dossier de crédit d'environ 1 400 personnes. [11]

Des organismes peuvent aussi sans le vouloir divulguer des renseignements personnels à des criminels qui se font passer pour des entreprises légitimes. C'est ce qui s'est passé au début de 2005 lorsque le courtier en information américain *ChoicePoint* a par inadvertance vendu les renseignements personnels d'au moins 145 000 Américains à 50 voleurs d'identité. [12]

De plus, certaines pratiques commerciales, par exemple l'impression du numéro d'assurance sociale sur les rapports de crédit ou l'envoi par la poste de demandes de crédit préapprouvées, encouragent les « vidangeurs » qui n'hésitent pas à fouiller dans les contenants à rebuts afin de trouver des données personnelles dont ils pourront ensuite se servir pour commettre des crimes.

Toutes ces pratiques trouvent un terrain fertile dans un marché hautement compétitif, dans lequel les consommateurs comptent de plus en plus sur le crédit pour effectuer des achats. Ce type de marché incite les prêteurs à accéder rapidement aux demandes de crédit à la consommation, et ils le font d'autant plus volontiers qu'aucune loi n'exige que les organismes prennent des mesures pour vérifier l'identité de la personne qui présente une demande de crédit.

En demandant aux prêteurs de faire preuve d'une plus grande vigilance au moment de vérifier l'identité des consommateurs, on pourrait réduire le nombre de vols d'identité. Certains prêteurs ne prennent pas assez de précautions lorsqu'ils vérifient l'identité d'un consommateur : ils craignent que, en posant trop de questions ou en tardant à répondre à une demande, les consommateurs se découragent et se tournent vers une autre entreprise. Les utilisateurs de cartes de crédit ou de téléphones cellulaires sont une assez bonne source de profit, et un certain nombre de sociétés émettrices préfèrent absorber les pertes qu'entraînent les vols d'identité occasionnels que de se passer des gains que ces consommateurs peuvent générer. [13] Selon les statistiques réunies par le Centre d'appel antifraude du Canada (PhoneBusters) pour 2003 et la première moitié de 2004, les plaintes liées au vol d'identité concernent le plus souvent l'utilisation d'une carte de crédit ou une demande frauduleuse de carte de crédit (32 %) ou l'utilisation d'un téléphone cellulaire ou la présentation d'une demande frauduleuse de téléphones cellulaires (10 à 12 %).

Même si les pertes subies par Visa et Mastercard s'élevaient à 134,10 millions de dollars en 1999 et à 163,18 millions de dollars en 2004, elles ne représentent qu'un faible pourcentage du volume des ventes générales des banques (moins de 1 %). [14] De toute façon, le prêteur n'assume pas seul toutes les pertes. Une partie de celles-ci doit être assumée par les victimes qui sont incapables de prouver qu'une fraude a été commise à leur endroit. Cette situation enchaîne un paradoxe où les consommateurs victimes du vol d'identité sont moins disposés à prévenir et absorber les pertes que les créditeurs. Les créditeurs quant à eux, trouvent qu'il est plus rentable de traiter les demandes de crédit que de poser des questions exploratoires afin d'authentiquer l'identité des demandeurs. [15]

De plus, les victimes doivent rétablir leur réputation, ce qui exige beaucoup de temps[16], et ce processus est angoissant et douloureux sur le plan émotionnel[17]. Les victimes ont aussi une réputation à rétablir : leurs mauvaises créances ont été enregistrées auprès des tribunaux, et leur cote de crédit s'est effondrée. Par ricochet, cette situation empêche les victimes de trouver un emploi ou d'obtenir du crédit lorsqu'elles en ont besoin. Il peut même arriver que les victimes possèdent un casier judiciaire si le fraudeur a été reconnu coupable d'une infraction en se faisant

passer pour la victime[18].

Pour trouver une solution efficace, il faut compter sur la collaboration des entreprises, des institutions financières, des bureaux de crédit, des consommateurs et des gouvernements. Ils ont tous un rôle à jouer pour garantir que les renseignements personnels ne sont pas accessibles aux voleurs d'identité qui veulent les utiliser à des fins criminelles.

Vue d'ensemble de la législation

Un certain nombre de lois fédérales, provinciales et territoriales traitent de façon fragmentée d'un aspect ou d'un autre du vol d'identité. Si l'on veut s'attaquer à l'ensemble du problème, il faut donc que les deux ordres de gouvernement prennent les mesures qui viseront plusieurs textes de loi différents. Pour cerner les solutions possibles, on a examiné les lois sur le vol d'identité adoptées en Europe, aux États-Unis et en Australie. De toute évidence, les législateurs américains ont été les plus actifs. Deux facteurs peuvent expliquer cela. En premier lieu, le vol d'identité est un problème plus important aux États-Unis qu'en Europe ou en Australie. En deuxième lieu, parmi les administrations examinées, celle des États-Unis est la seule à ne pas avoir de lois d'ensemble visant à protéger les données.

Lois sur la protection des renseignements personnels

La *Loi sur la protection des renseignements personnels et les documents électroniques* (LPRPDE) du gouvernement fédéral régit la collecte, l'utilisation et la divulgation des renseignements personnels par les entreprises. Le Québec, la Colombie-Britannique et l'Alberta ont adopté des lois semblables, en substance, pour protéger les renseignements personnels, et elles s'appliquent aux organismes qui y sont assujettis. Les renseignements personnels qui traversent les frontières internes à des fins commerciales sont aussi assujettis à la LPRPDE. Ces lois sur la protection des renseignements personnels exigent que les organismes avisent les particuliers des raisons pour lesquelles ils ont besoin des informations et qu'ils ne les recueillent pas sans leur consentement, sauf dans les cas où la loi autorise la collecte d'informations sans consentement. Les organismes doivent aussi ne recueillir que les informations dont ils ont raisonnablement besoin, et ne les utiliser et les divulguer qu'aux fins indiquées ou aux fins précisées par la loi. Les organismes doivent aussi veiller à ce que les informations soient exactes et protégées et ne doivent les conserver qu'aussi longtemps qu'il est nécessaire aux fins indiquées. Les particuliers doivent pouvoir accéder aux informations et les corriger, sauf dans les cas prescrits par la loi. Enfin, les organismes sont responsables des informations qu'ils détiennent, et les particuliers peuvent déposer une plainte auprès d'un commissaire à la protection de la vie privée indépendant habilité à mener des enquêtes et à tenter de régler les plaintes. Les commissaires de l'Alberta, de la Colombie-Britannique et du Québec ont le pouvoir d'émettre des ordonnances exécutoires. La loi fédérale permet que les différends non réglés qui concernent certaines questions soient portés devant la Cour fédérale.
Il convient aussi de signaler que l'Ontario, le Manitoba, la Saskatchewan et l'Alberta se sont

aussi dotées de lois sur la protection des renseignements sur la santé fondées sur les principes d'équité en matière d'information qui ont été présentés ci-dessus et qui peuvent s'appliquer à certaines entreprises.

Lois fédérales

On pourrait utilement s'inspirer de la *LPRPDE* et de la *Loi sur les banques*, loi fédérale, au moment d'étudier certaines des réformes proposées. On peut aussi s'inspirer d'autres lois visant un secteur spécifique. Il faudra mener des analyses juridiques plus poussées pour déterminer en quoi ces lois pourraient être touchées.

Le gouvernement fédéral a aussi élaboré un ensemble de directives facultatives à l'intention des organismes qui doivent garantir l'identité d'un intervenant du cybermarché[19]. Même si ces *Principes d'authentification électronique* n'ont pas force de loi, ils constituent des balises en permettant de garantir que le processus d'authentification est fondé sur des pratiques commerciales saines réalisant l'équilibre entre les avantages du commerce électronique et les risques pour les consommateurs. Ces principes doivent en particulier garantir que l'attribution doit être « raisonnable et juste et tenir compte de la capacité des parties prenantes de gérer les risques ou d'absorber les pertes ». Ils devraient aussi inciter les parties chargées de l'élaboration et de la mise en œuvre des processus d'authentification à voir à ce que leurs produits et leurs services soient sûrs et fiables[20].

Le *Code criminel du Canada* comprend des dispositions relatives aux infractions traditionnelles que constituent la fraude et le vol ou encore le trafic des données sur les cartes de crédit ou l'interférence visant les données. Au cours des dernières deux années, Justice Canada a analysé les restrictions du Code au sujet du vol d'identité et étudie une variété d'options pour affronter le problème.

Lois provinciales

Les lois provinciales et territoriales énoncent les règles et les responsabilités des bureaux de crédit qui possèdent des dossiers d'information sur le crédit de personnes. Les lois sur les renseignements concernant les consommateurs protègent aussi la vie privée de ces derniers en ce qui concerne les renseignements sur le crédit et leur droit de ne pas voir leurs transactions financières menacées en raison de l'inexactitude de renseignements sur le crédit ou de renseignements personnels figurant dans leur dossier. C'est pourquoi toutes les provinces, exception faite du Nouveau-Brunswick, ont adopté des lois sur les renseignements sur le crédit des consommateurs. Ces lois s'appliquent aux grands bureaux de crédit (Equifax, TransUnion, Northern Credit Bureau) et aux autres entités commerciales qui possèdent des bases de données sur le crédit personnel ou des renseignements concernant le crédit. Dans le présent document, les options qui concernent les bureaux de crédit ou les agences de renseignements sur la consommation s'appliquent à tous les organismes assujettis aux lois sur les renseignements

concernant le consommateur. Les provinces et territoires ont aussi compétence sur les coopératives d'épargne et de crédit, les Caisses populaires et certaines sociétés de fiducie.

Il existe aussi des lois provinciales et territoriales sur la protection des consommateurs qui ont en général pour objectif de protéger les consommateurs dans le marché et d'assurer aux entreprises des règles du jeu équitables. Les lois déterminent le type de renseignements qui peuvent être divulgués aux consommateurs selon la transaction, les cas où on doit prévoir une période pendant laquelle les consommateurs peuvent réfléchir à leurs décisions ainsi que les recours qui s'offrent aux consommateurs lorsqu'une transaction visant un bien ou un service est erronée.

Lois américaines

Un certain nombre d'administrations des États-Unis ont adopté des lois sur le vol d'identité. Ces lois comprennent certaines dispositions qui pourraient s'appliquer au Canada, et c'est pourquoi on a jugé utile de les examiner.

La loi la plus complète a été adoptée par le gouvernement américain en 2003. Il s'agit de la *Fair and Accurate Credit Transactions Act* (FACTA) que l'on pourrait traduire par Loi sur l'équité et l'exactitude en matière de transactions de crédit. La FACTA permet aux consommateurs d'exercer un contrôle plus serré sur leurs rapports de crédit et leur donne même le droit de faire inscrire un avertissement de fraude sur leur dossier de crédit dans le cas où des renseignements personnels les concernant ont été compromis. Les consommateurs peuvent aussi empêcher que des renseignements erronés les concernant (qui découlent d'un vol d'identité) soient divulgués à des créanciers, et ils peuvent obtenir gratuitement, chaque année, une copie de leur rapport de crédit. D'autres dispositions exigent que les numéros des cartes de paiement qui figurent sur les reçus soient tronqués, et que le calcul de la cote de crédit soit plus transparent aux yeux des consommateurs.

De plus, un certain nombre d'États américains – notamment la Californie, l'Illinois, le Texas, la Louisiane, l'Arizona et le Connecticut – ont modifié leurs lois sur la protection des consommateurs et les renseignements concernant le consommateur pour ajouter des mesures visant à limiter les vols d'identité sur leur territoire respectif[21]. Bon nombre des dispositions de ces lois se retrouvent dans la FACTA; mais il existe des mesures supplémentaires. Par exemple, dans certains États, les créanciers doivent vérifier s'il y a eu changement d'adresse avant d'envoyer une demande de crédit préapprouvée, les bureaux de crédit doivent vérifier l'identité des personnes désirant obtenir un rapport de crédit ou encore les organismes doivent aviser les consommateurs lorsqu'il y a bris de sécurité concernant leurs renseignements personnels.

Régler le problème – Solutions possibles

Dans la section suivante, on expose un certain nombre d'options de réforme législative. On peut recourir à deux types de mécanisme pour mettre en œuvre les options décrites en détail plus loin. Un mécanisme serait l'adoption d'une nouvelle loi autonome réunissant les diverses mesures de lutte contre le vol d'identité (p. ex. la Loi sur les moyens de lutter contre le vol d'identité). L'autre mécanisme viserait l'adoption d'une loi modifiant d'autres lois, qui permettrait tout simplement de modifier des lois existantes. Pour mettre en œuvre les options proposées, il faudrait probablement modifier les lois suivantes :

a) des lois fédérales comme la *LPRPDE*;

b) des lois provinciales et territoriales visant les renseignements concernant le consommateur, la protection des consommateurs, les coopératives d'épargne et de crédit et les caisses populaires, les compagnies d'assurances, les sociétés de prêt, les sociétés de fiducie et les municipalités, ainsi que les lois sur la protection des renseignements personnels et les renseignements sur la santé semblables à la LPRPDE.

Quel que soit le véhicule choisi, les mesures législatives devront être adoptées à l'échelle fédérale de même qu'à l'échelle provinciale et territoriale afin de mettre en œuvre les options proposées.

On a divisé les options en trois catégories. La première comprend les réformes visant à faire en sorte qu'il soit plus difficile pour les voleurs d'identité de mettre la main sur des renseignements personnels. La seconde s'attache aux réformes visant à faciliter le contrôle ou la constatation précoce du vol d'identité. La troisième comprend les réformes visant à faciliter, pour les victimes, le processus d'indemnisation.

(1) Empêcher les fuites

Option I – Tronquer (cacher partiellement) le numéro des cartes de paiement

> *Les personnes qui acceptent des cartes de paiement (les cartes de crédit et les cartes de débit) pour une transaction commerciale ne doivent pas imprimer la date d'expiration non plus que les cinq derniers chiffres du numéro de la carte sur un reçu généré électroniquement au point où s'effectue la vente ou la transaction.*

Cette option permettrait de limiter le volume des renseignements personnels qui sont rendus accessibles de façon routinière dans le cadre d'opérations commerciales ordinaires. Le numéro de compte et la date d'expiration sont des renseignements qui facilitent de toute évidence la fraude surtout lorsque les voleurs d'identité peuvent les utiliser, avec le nom de la personne visée, pour effectuer des transactions bancaires ou des achats frauduleux. Le numéro d'une carte de débit est probablement moins vulnérable, puisqu'il suppose l'utilisation d'un NIP, mais en limitant la divulgation des numéros de carte de débit, on complique encore plus l'obtention par les voleurs d'identité de données essentielles sur une personne.

En tronquant automatiquement le numéro de carte de paiement figurant sur un reçu, on favorise aussi l'adoption de bonnes pratiques en matière de renseignements puisqu'on met en relief l'importance de la protection des renseignements personnels sans rien enlever à l'utilité du reçu imprimé. En limitant le type d'information qui figure sur un reçu, cette option met des bâtons dans les roues aux « vidangeurs » et protège le numéro de la carte de paiement au point où s'effectue la transaction ou la vente. On peut quand même utiliser le reçu imprimé pour vérifier la transaction, au besoin, puisque le titulaire de la carte possède encore le numéro complet nécessaire aux fins d'authentification.

Cette option a été adoptée dans un certain nombre d'États américains, y compris l'Arizona, l'Illinois et la Californie, de même qu'à l'échelle fédérale, par le truchement de la FACTA. Les lois de la Californie et de l'Arizona visent uniquement les numéros des cartes de crédit, mais dans d'autres États, les dispositions visent aussi les numéros des cartes de débit. En vertu de toutes ces lois, le défaut de respecter ces dispositions équivaut à une pratique commerciale illégale pouvant donner lieu à des pénalités.

De plus, les législateurs américains ont limité l'application de cette disposition au reçu imprimé électroniquement et en ont exclu de façon expresse les reçus écrits à la main et les cartes imprimées. La disposition prévoit donc des exemptions pour les très petites entreprises ou les utilisateurs occasionnels du système de carte de crédit (par exemple les chauffeurs de taxi indépendants) qui ne sont pas toujours en mesure d'absorber le coût d'un système de paiement électronique. Les législateurs ont en outre presque toujours reporté de deux ou trois ans l'application de cette disposition dans les cas où une entreprise est déjà en exploitation au moment où la loi est adoptée de façon à lui donner le temps de remplacer ou de modifier son équipement.

Au Canada, bon nombre de grands détaillants ont adopté cette pratique de façon volontaire. D'autres entreprises, en particulier les petites entreprises, n'ont pas commencé à tronquer les numéros des cartes de paiement parce que le remplacement ou la modification de l'équipement suppose des coûts. On pourrait atténuer le problème en incluant une clause de droits acquis – autrement dit, les petits détaillants ne seraient obligés de respecter cette disposition qu'au moment où ils remplacent leur équipement par les nouveaux systèmes d'information. Autrement, on pourrait reporter de deux ou trois ans l'application de la disposition dans le but de permettre aux organismes d'absorber les coûts connexes.

Cette option est conforme aux pratiques commerciales actuelles, les sociétés de carte de crédit ayant déjà tendance à tronquer les numéros.

QUESTIONS POUR L'OPTION I

1. Pensez-vous que cette option assurerait une meilleure protection contre le vol d'identité?
   - Oui ou non
   - Veuillez expliquer pourquoi.
2. Quels seraient les coûts de cette option? Permettrait-elle des économies compensatoires? Qui devrait assumer les coûts?
3. Devrait-on prévoir des exceptions? Si oui, lesquelles?
4. Faudrait-il que cette disposition soit associée à des pénalités? (tel que proposé à l'option 9)
5. Pour cette option, qui serait le premier responsable des pertes associées au vol d'identité?
6. Cette option comporte-t-elle des désavantages pour les consommateurs ou l'industrie? Veuillez fournir des détails.
7. Quelles sont les normes actuelles ou projetées de l'industrie en ce qui concerne la troncation des cartes de paiement? Quel en est le calendrier de mise en œuvre? Les normes excluent-elles les reçus écrits à la main et les cartes imprimées?

Option II – Vérifier l'identité des personnes et des organismes qui ont accès aux rapports de crédit

Les bureaux de crédit doivent prendre des mesures raisonnables pour établir l'identité des personnes et des organismes qui accèdent aux rapports de crédit.

Le rapport de crédit d'une personne contient un assez grand nombre de renseignements personnels : nom, âge, situation de famille, nom et âge du conjoint, nombre de personnes à charge, détails concernant la scolarité ou les compétences professionnelles, adresse actuelle et adresses précédentes, numéro d'assurance sociale, numéro de téléphone, date de naissance, antécédents professionnels, revenu estimé, habitudes de paiement, dettes, obligations relatives au coût de la vie, actifs. Il est clair que ces renseignements sont utiles pour les voleurs d'identité. Lorsqu'un rapport est vendu à des personnes non autorisées, le préjudice causé à la personne visée est important puisque ce rapport fournit plus d'information qu'il n'est nécessaire pour endosser l'identité de cette personne. De plus, un voleur d'identité peut tenter d'obtenir une copie du rapport de crédit d'un consommateur en se faisant passer pour lui.

Dans la plupart des provinces et territoires, la loi interdit à quiconque d'obtenir le rapport d'un consommateur sans le consentement de ce dernier ou sans que le consommateur n'ait été avisé par écrit du fait qu'un rapport sera transmis. Les lois exigent aussi que les bureaux de crédit aient une raison de croire que le rapport a été demandé à des fins légitimes. Cette option obligerait les bureaux de crédit à prendre des mesures raisonnables pour vérifier l'identité des personnes qui demandent un rapport de crédit afin de garantir qu'elles sont bien les personnes qu'elles prétendent être.

En interdisant la divulgation d'un rapport de crédit à des personnes non autorisées, on réduirait de beaucoup le vol d'identité puisque l'on pourrait protéger le caractère confidentiel des

renseignements personnels contenus dans ce rapport et compliquer énormément la tâche des voleurs qui veulent obtenir du crédit en utilisant le nom d'un consommateur. En imposant des pratiques normalisées en matière d'authentification, on uniformise les règles du jeu dans le secteur privé en incitant les gens à garantir que les processus d'authentification sont sûrs et fiables et qu'ils sont conformes aux *Principes d'authentification électronique* du gouvernement fédéral[22].

QUESTIONS POUR L'OPTION II

1. Pensez-vous que cette option assurerait une meilleure protection contre le vol d'identité?
2. Quels seraient les coûts de cette option? Permettrait-elle des économies compensatoires? Qui devrait assumer les coûts?
3. Devrait-on prévoir des exceptions? Si oui, lesquelles?
4. Faudrait-il que cette disposition soit associée à des pénalités?
5. Pour cette option, qui serait le premier responsable des pertes associées au vol d'identité?
6. Cette option comporte-t-elle des désavantages pour les consommateurs ou l'industrie? Veuillez fournir des détails.
7. Est-ce que les obligations relatives à l'authentification doivent aussi être imposées aux intervenants du marché de la revente des rapports de crédit? Si vous pensez que non, veuillez fournir vos raisons.
8. Les bureaux de crédit fournissent-ils différents niveaux d'information en fonction des besoins de l'organisme ou de la personne qui demande le rapport de crédit? Dans le cas échéant, quelles normes s'appliquent?
9. Quel serait le coût de l'authentification pour les fournisseurs de crédit et pour les consommateurs?

Option III – Ne pas inscrire le numéro d'assurance sociale (NAS) sur les rapports de crédit ni l'utiliser comme code d'identification unique des consommateurs.

> *Lorsqu'il est pertinent que les institutions financières enregistrent le NAS, elles devraient en protéger le caractère confidentiel. En particulier, les agences de renseignements sur la consommation et les institutions financières ne devraient pas utiliser le NAS comme code d'identification unique des consommateurs ni inscrire ce numéro sur un rapport de crédit.*

Même si, selon la loi, une personne n'a pas à divulguer son numéro d'assurance sociale, sauf dans le cas d'un nombre limité de programmes gouvernementaux, de nombreux organismes – y compris les institutions financières et les bureaux de crédit – utilisent le NAS comme méthode pratique de vérifier l'identité d'une personne. Puisque le NAS n'appartient qu'à une seule personne, un prêteur, par exemple, peut en toute confiance prendre une décision concernant un

prêt en se fondant sur le rapport de crédit puisqu'il sait que ce rapport concerne la personne qui demande le prêt. Le NAS est donc un code d'identification pratique, fréquemment utilisé pour les activités commerciales, spécialement pour les transactions de crédit.

Toutefois, l'utilisation du NAS par les entreprises cause des inquiétudes particulières puisque ce numéro est une clé qui permet aux voleurs d'identité d'entrer dans la vie de la victime[23]. Avec le nom et le NAS d'une personne, un voleur d'identité peut demander des prestations gouvernementales, signer un bail, obtenir un prêt ou travailler sous le nom de sa victime. Protéger le NAS serait donc un moyen efficace de réduire le volume de données de nature délicate auxquelles ont accès les voleurs d'identité.

Le Bureau du vérificateur général indiquait en 2002 que le fait que d'autres ordres de gouvernement et des institutions utilisent de plus en plus le NAS augmente à la fois les possibilités de fraude à partir du NAS et leurs répercussions. Par exemple, une personne qui obtient de façon frauduleuse une fausse identité, y compris une carte portant le NAS délivrée par DRHC, peut utiliser cette identité pour accéder à des programmes sociaux fédéraux, provinciaux et territoriaux, frauder les banques ou fournir de fausses déclarations de revenu à l'Agence des douanes et du revenu du Canada[24].

Cette option permettrait de protéger le caractère confidentiel des NAS en interdisant aux bureaux de crédit d'inscrire le NAS d'une personne sur son rapport de crédit. Les institutions financières et les bureaux de crédit seraient en outre obligés de créer un autre code d'identification unique des consommateurs. Un NAS tronqué serait peut-être une solution acceptable.

Il n'existe pas de mesure de protection équivalente dans d'autres administrations; cependant, la FACTA prévoit que les consommateurs peuvent demander que le numéro de sécurité sociale qui figure sur leur rapport de crédit soit tronqué. Cela signifie que les consommateurs avisés pourront obtenir une protection supplémentaire, mais la plupart des personnes resteront sans protection.

Cette option entraînerait une augmentation des coûts de mise en œuvre d'un nouveau code d'identification imposés au bureau de crédit et aux institutions financières. Cela pourrait aussi compliquer la vérification des antécédents de crédit d'une personne. Cela pourrait aussi empêcher les organismes prêteurs de vérifier aussi facilement le crédit des personnes qui, de manière légitime, présentent une demande de crédit. On ne sait pas encore si les consommateurs seront prêts à accepter les délais que cette option suppose.

QUESTIONS POUR L'OPTION III

1. Pensez-vous que cette option assurerait une meilleure protection contre le vol d'identité? Pourquoi/pourquoi pas?
2. Quels seraient les coûts de cette option? Permettrait-elle des économies compensatoires? Qui devrait assumer les coûts?
3. Devrait-on prévoir des exceptions? Si oui, lesquelles?
4. Faudrait-il que cette disposition soit associée à des pénalités?
5. Pour cette option, qui serait le premier responsable pour les pertes associées au vol d'identité?
6. Cette option comporte-t-elle des désavantages pour les consommateurs ou l'industrie? Veuillez fournir des détails.
7. Les institutions financières se sont-elles dotées d'une norme concernant la divulgation du NAS? Dans le cas échéant, dans quels cas demandent-elles le NAS? Y a-t-il des zones grises?
8. Les compagnies de télécommunications, les agences immobilières et les détaillants se conforment-ils à une norme concernant la divulgation du NAS?
9. Combien coûterait l'élaboration d'un code d'identification unique? Combien de temps faudrait-il pour le mettre en œuvre?
10. Est-ce que la troncation du NAS serait la meilleure solution? Dans ce cas, comment pourrait-on la mettre en œuvre?

(2) Soutenir la détection

Option IV – Permettre aux consommateurs de bloquer leurs rapports de crédit.

> *Sur demande du consommateur, les bureaux de crédit doivent bloquer, gratuitement, la divulgation de son rapport de crédit. Lorsque le blocage existe, le bureau de crédit ne peut transmettre le rapport de crédit à un tiers sans avoir obtenu au préalable l'autorisation expresse du consommateur. Pour obtenir cette autorisation, le bureau de crédit devra communiquer avec le consommateur à une adresse civique ou un numéro de téléphone prédéterminés.*

Une mesure de blocage permettrait aux consommateurs qui se préoccupent du vol d'identité d'ordonner à un bureau de crédit de ne pas divulguer leur rapport de crédit sans d'abord obtenir leur autorisation expresse. Puisque les consommateurs doivent être avisés chaque fois qu'une personne demande d'obtenir le rapport de crédit les concernant, ils pourraient découvrir qu'une demande de crédit est faite de manière frauduleuse.

Cette option permettrait donc aux consommateurs d'exercer un contrôle plus serré sur la façon

dont on utilise ou transmet des renseignements personnels les concernant et que détiennent les bureaux de crédit. Elle ferait aussi en sorte qu'ils seraient avisés lorsqu'une personne non autorisée demande leur rapport de crédit. Il serait donc beaucoup plus difficile pour un voleur d'identité d'obtenir du crédit sous un autre nom.

Les blocages de sécurité ont été imposés par la loi en Californie, en Louisiane et au Texas. Le consommateur qui demande le blocage doit fournir des pièces d'identité appropriées, et le bureau de crédit doit mettre le blocage en vigueur avant l'échéance d'un certain délai (de 24 heures à cinq jours). Le bureau de crédit doit aussi faire parvenir au consommateur, au plus 10 jours plus tard, un mot de passe ou un numéro d'identification personnel grâce auquel le consommateur pourra autoriser la transmission d'un rapport ou lever temporairement l'ordre de blocage. Les bureaux de crédit qui ne se conforment pas à cette disposition – sciemment ou par négligence – peuvent se voir imposer des pénalités allant de 500 $ à 2 500 $, auxquelles s'ajoutent les frais juridiques.

Si le mot de passe est posté après coup au consommateur, il peut être subtilisé par un voleur d'identité, surtout si l'adresse qui figure au dossier a été compromise. C'est pourquoi, selon cette option, le bureau de crédit devra utiliser un numéro de téléphone déterminé d'avance afin de demander au consommateur son autorisation. Puisque le numéro aura été déterminé avant la demande de gel du crédit, il sera plus difficile, pour un voleur, de prendre le contrôle d'un compte.

Selon cette option, tous les consommateurs devraient avoir le droit de demander le gel de leur crédit, sans frais, ce qui garantirait un niveau de protection minimum pour tous. Elle est en outre conforme aux principes de l'authentification, selon lequel l'attribution des risques doit tenir compte de la capacité des parties prenantes de gérer les risques ou d'absorber les pertes.

QUESTIONS POUR L'OPTION IV

1. Pensez-vous que cette option assurerait une meilleure protection contre le vol d'identité? Pourquoi/pourquoi pas?
2. Quels seraient les coûts de cette option? Permettrait-elle des économies compensatoires? Qui devrait assumer les pertes?
3. Devrait-on prévoir des exceptions? Si oui, lesquelles?
4. Faudrait-il que cette disposition soit associée à des pénalités?
5. Pour cette option, qui serait le premier responsable pour les pertes associées au vol d'identité?
6. Cette option comporte-t-elle des désavantages pour les consommateurs ou l'industrie? Veuillez fournir des détails.
7. S'agirait-il d'un instrument de prévention ou d'un recours à la suite d'un vol?
8. Cette option aura-t-elle une incidence sur le contrôle de la solvabilité ou sur d'autres activités de marketing?

9. Y aurait-il des exceptions au gel des rapports de crédit?
10. Devrait-on imposer des frais raisonnables pour recouvrer les coûts de ce service?

Option V – Exiger que les organismes qui possèdent des renseignements personnels sur d'autres personnes avisent celles-ci ainsi que les bureaux de crédit en cas de bris de sécurité.

> *En cas de bris de sécurité des renseignements personnels détenus par un organisme, celui-ci devra communiquer avec les personnes dont les renseignements personnels sont compromis et avec les bureaux de crédit concernés, aussi rapidement qu'il est possible de le faire.*

On ne sait pas si le marché peut fournir suffisamment de motifs incitant les organismes à renseigner les particuliers lorsqu'il y a eu bris de sécurité de leurs renseignements personnels; il est possible que des personnes ne soient pas avisées du fait qu'elles présentent un risque élevé de vol d'identité. Les personnes peu méfiantes ne pourront donc pas prendre de mesures correctives rapidement.

Selon cette option, un organisme qui a fait l'objet d'un bris de sécurité sera obligé de renseigner toutes les personnes concernées et d'assumer les coûts de ces communications. Dans l'affaire ChoicePoint, on a vu que les lois qui exigent la notification d'un bris de sécurité ont des répercussions directes sur le comportement des entreprises. ChoicePoint a avisé les résidents de la Californie du fait que des renseignements personnels les concernant avaient été transmis à des personnes non autorisées; l'entreprise a agi ainsi parce qu'elle y était obligée en vertu des lois californiennes. Elle n'a pas avisé les personnes qui n'étaient pas des résidents de la Californie, puisque la loi ne l'exigeait pas, mais s'est ravisée sous la pression assez forte des médias.

Au Canada, le bureau Equifax et la société d'assurance-vie Co-operators ont subi des bris de sécurité, et il semble qu'elles aient tardé à aviser les consommateurs concernés. Les dispositions législatives visant le devoir d'aviser seraient probablement assez efficaces et garantiraient que les victimes potentielles d'un vol d'identité seront avisées rapidement en cas de bris de sécurité.

Cette option serait en outre conforme aux pratiques équitables en matière de renseignements énoncées dans la LPRPDE et les lois provinciales. Puisque les organismes doivent garantir la sécurité des renseignements personnels, on pourrait faire en sorte, en exigeant que l'on avise les personnes en cause, que les organismes qui ne se conforment pas à cette disposition restent responsables devant ces personnes.

Selon cette option, on pourrait aussi exiger que les organismes transmettent aux bureaux de crédit pertinents le nom de toutes les personnes dont les renseignements personnels ont été

compromis, de façon que ces bureaux ajoutent un avertissement de fraude à leurs dossiers de crédit (voir l'option 6 ci-dessous).

Si la loi obligeait les organismes à aviser les bureaux de crédit pertinents, il faudrait que la LPRPDE et les lois provinciales les autorisent à divulguer des renseignements personnels sans le consentement et à l'insu des personnes concernées. Toutefois, afin de pallier tout préjudice potentiel, les organismes seraient aussi obligés d'aviser ces personnes du fait qu'un avertissement de fraude a été ajouté à leur dossier de crédit (voir l'analyse de l'option 6, ci-dessus).

QUESTIONS POUR L'OPTION V

1. Pensez-vous que cette option assurerait une meilleure protection contre le vol d'identité?
2. Quels seraient les coûts de cette option? Permettrait-elle des économies compensatoires? Qui devrait assumer les coûts?
3. Devrait-on prévoir des exceptions? Si oui, lesquelles?
4. Faudrait-il que cette disposition soit associée à des pénalités?
5. Pour cette option, qui serait le premier responsable des pertes associées au vol d'identité?
6. Cette option comporte-t-elle des désavantages pour les consommateurs ou l'industrie? Veuillez fournir des détails.
7. Existe-t-il des éléments du marché, par exemple des obligations contractuelles, qui exigent que les organismes déclarent qu'elles ont été victimes d'un bris de sécurité? Dans le cas échéant, quels sont-ils? Visent-ils uniquement la compromission de certains types de renseignements, par exemple les renseignements de nature financière?
8. En tant que consommateur, seriez-vous prêt à renoncer à une partie du contrôle que vous exercez sur vos renseignements personnels pour permettre à une entreprise de prendre rapidement des mesures de protection contre le vol d'identité et de demander à votre bureau de crédit d'ajouter un avertissement de fraude à votre dossier?
9. À partir de quel moment les consommateurs devraient-ils être avisés lorsque les renseignements personnels les concernant ont été compromis?
10. Quel délai les entreprises devront-elles respecter pour aviser les consommateurs et quels moyens devraient-elles utiliser?
11. Devrait-on intégrer à cette proposition une disposition selon laquelle des organismes seraient obligés d'aviser le Centre d'appels antifraude?
12. Serait-ce une bonne approche pour la mise sur pied d'un organisme centralisé de signalement, qui cernera les tendances et compilera des statistiques plus précises?

Option VI – Exiger que les bureaux de crédit ajoutent un avertissement de fraude aux rapports de crédit des consommateurs lorsqu'il y a eu un bris de sécurité ou lorsqu'une victime d'un vol d'identité le demande.

> *Après avoir été avisé par un organisme que la sécurité des renseignements personnels d'une victime a été violée ou sur demande d'une victime de vol d'identité, un bureau de crédit devra ajouter un avertissement de fraude au rapport de crédit des consommateurs visés pour indiquer qu'il est possible que l'on ait utilisé leur identité, sans leur consentement, pour obtenir de façon frauduleuse des biens ou des services. Un créancier qui reçoit un rapport de crédit comportant cet avertissement ne pourra accorder un crédit à une personne ni augmenter le montant de son crédit sans d'abord prendre des mesures raisonnables pour vérifier l'identité de la personne qui présente la demande.*

À l'heure actuelle, une entreprise qui est victime d'un bris de sécurité peut, si elle le veut, aviser les consommateurs concernés. Elle leur envoie une lettre leur conseillant de communiquer avec leurs bureaux de crédit afin d'évaluer s'il est nécessaire d'émettre un avertissement de fraude. Des consommateurs doivent alors communiquer avec les bureaux de crédit pour obtenir le formulaire par lequel ils pourront demander qu'un avertissement de fraude soit versé à leur dossier. Ce processus suppose de longs délais, et des préjudices peuvent être causés pendant cette période. On pourrait simplifier le processus de façon qu'une entreprise soit obligée d'aviser les bureaux de crédit pour demander qu'un avertissement de fraude soit versé immédiatement au dossier. Le consommateur pourrait être avisé de l'infraction, le plus rapidement qu'il est possible de le faire, pour que celui-ci décide s'il veut supprimer l'avertissement.

Lorsque des renseignements personnels sont divulgués sans autorisation, les créanciers potentiels n'ont aucun moyen de savoir que les informations sur lesquelles ils se fondent pourraient être entre les mains d'un voleur d'identité. Cette option permettrait de garantir qu'un avertissement de fraude est versé au dossier de crédit d'une personne lorsqu'il y a eu fuite de renseignements personnels. Les créanciers potentiels pourraient ainsi savoir qu'il y un risque de vol d'identité. En conséquence, ils n'auraient pas le droit de consentir un crédit tant qu'ils n'auront pas communiqué avec le consommateur en utilisant un numéro de téléphone prédéterminé afin d'obtenir leur autorisation.

Une disposition semblable est intégrée à la FACTA et aux lois de la Californie, de la Louisiane et du Texas. Selon la FACTA, une personne ne peut demander que l'on ajoute un avertissement de fraude à son dossier que si elle croit avoir été victime d'un vol d'identité ou si elle croit qu'elle pourrait l'être bientôt. Trois administrations prévoient que l'avertissement doit rester au dossier pendant 90 jours (45 jours pour le Texas), mais toutes les quatre permettent à une personne de le renouveler. La FACTA indique que, lorsqu'un consommateur signale un vol d'identité, l'avertissement demeure en vigueur pendant sept ans.

Les lois américaines exigent aussi que les bureaux de crédit offrent un service d'aide sans frais, 24 heures sur 24 et sept jours sur sept, et qu'ils consignent les demandes d'avertissement de fraude. De cette manière, on garantit qu'une personne peut communiquer rapidement avec le bureau de crédit concerné afin de protéger son rapport de crédit dès qu'elle apprend que ses renseignements personnels ne sont plus protégés. En outre, les bureaux de crédit qui, sciemment ou par négligence, ne prennent pas les mesures nécessaires lorsqu'une personne demande que l'on ajoute cet avertissement peuvent se voir imposer des pénalités de 500 $ à 2 500 $.

On pourrait renforcer cette option en exigeant que des bureaux de crédit offrent un service d'aide sans frais de façon à consigner les demandes d'avertissement de fraude et en imposant des pénalités pour le défaut de se conformer. On pourrait aussi imposer des pénalités aux institutions financières qui accordent du crédit sans d'abord vérifier l'identité du consommateur, par exemple, en lui téléphonant à un numéro de téléphone prédéterminé.

Selon cette option, on pourrait ajouter un avertissement de fraude aux rapports de crédit des consommateurs sans qu'ils en soient avisés. Toutefois, on pourrait réduire au minimum les préjudices causés en avisant les consommateurs par la suite, le plus rapidement qu'il est possible et raisonnable de le faire.

Il est difficile de déterminer qui sera responsable des coûts de cet avertissement, lorsqu'il est demandé par un organisme qui a subi une brèche de la sécurité – est-ce à l'organisme ou au bureau de crédit d'assumer les coûts? Cependant, lorsqu'une personne demande qu'un avertissement soit versé à son dossier, il ne devrait pas en assumer les coûts : on garantit ainsi un niveau de protection minimal pour tous les consommateurs. Encore une fois, cette option est conforme au principe en vertu duquel le risque doit être attribué à ceux qui sont les plus aptes à gérer les risques ou absorber les pertes.

QUESTIONS POUR L'OPTION VI

1. Pensez-vous que cette option assurerait une meilleure protection contre le vol d'identité? Pourquoi/pourquoi pas?
2. Quels seraient les coûts de cette option? Permettrait-elle des économies compensatoires? Qui devrait assumer les coûts?
3. Devrait-on prévoir des exceptions? Si oui, lesquelles?
4. Faudrait-il que cette disposition soit associée à des pénalités?
5. Pour cette option, qui serait le premier responsable des pertes associées au vol d'identité?
6. Cette option comporte-t-elle des désavantages pour les consommateurs ou l'industrie? Veuillez fournir des détails.

3) Rétablissement après le préjudice

Option VII – Exiger que les créanciers divulguent les détails des dettes frauduleuses aux victimes.

Les créanciers doivent fournir sur demande aux victimes d'un vol d'identité les détails concernant les dettes frauduleuses contractées en leur nom.

Afin de pouvoir rétablir leur réputation, les victimes ont souvent besoin des détails concernant les dettes frauduleuses contractées en leur nom. Par exemple, les victimes pourraient avoir besoin d'une copie de la demande de crédit signée afin de prouver qu'il y a eu contrefaçon. Ces informations sont nécessaires à diverses étapes, même avant qu'un rapport de police ait été rédigé.

Les créanciers sont souvent réticents à divulguer ces informations parce qu'ils hésitent à admettre une faute ou une responsabilité. Même si les particuliers ont, de façon générale, le droit d'accéder aux renseignements les concernant en vertu des lois sur la protection des renseignements personnels, il est possible que cet accès soit refusé pendant une enquête policière. Selon cette disposition, les créanciers seraient obligés de divulguer ces renseignements, même si une enquête est en cours.

Selon cette option, un créancier qui a accordé du crédit à un voleur d'identité utilisant le nom d'une victime devrait fournir à cette victime toutes les informations qu'il possède au sujet de la dette de façon que la victime puisse pallier les préjudices subis et protéger sa réputation.

Une disposition semblable est intégrée à la FACTA et aux lois de la Louisiane. Selon cette disposition, la victime doit fournir des preuves d'identité et prouver qu'il y a eu crime visant son identité. Elle pourra pour cela fournir au créancier une copie du rapport de police ainsi qu'une déclaration sous serment normalisée concernant le vol d'identité.

QUESTIONS POUR L'OPTION VII

1. Pensez-vous que cette option assurerait une meilleure protection contre le vol d'identité? Pourquoi/pourquoi pas?
2. Quels seraient les coûts de cette option? Permettrait-elle des économies compensatoires? Qui devrait assumer les coûts?
3. Devrait-on prévoir des exceptions? Si oui, lesquelles?
4. Faudrait-il que cette disposition soit associée à des pénalités?
5. Pour cette option, qui serait le premier responsable des pertes associées au vol d'identité?
6. Cette option comporte-t-elle des désavantages pour les consommateurs ou l'industrie? Veuillez fournir des détails.

Option VIII – Exiger que les bureaux de crédit bloquent les informations concernant les dettes frauduleuses qui figurent sur le rapport de crédit d'un consommateur.

> *Sur réception d'une preuve du vol d'identité, un bureau de crédit doit bloquer les informations sur les dettes contractées au nom d'un consommateur par un voleur d'identité de façon qu'elles ne figurent pas dans le rapport de crédit du consommateur. Le bureau de crédit pourra, dans certains cas, refuser de le faire ou annuler le blocage. Dans ce cas, il devra aviser le consommateur de sa décision à en fournissant les motifs.*

Les victimes d'un vol d'identité affirment qu'il est souvent difficile de corriger leur rapport de crédit. Selon cette option, les bureaux de crédit seraient obligés de bloquer les renseignements qui concernent les créances douteuses contractées par un voleur d'identité qui utilise le nom d'un consommateur. Ils devraient le faire après qu'un consommateur les a avisés de la situation de la façon appropriée. Toutefois, le bureau de crédit pourrait annuler le blocage s'il a des motifs raisonnables de croire que le consommateur a déguisé les faits.

La FACTA exige que, pour que les informations soient bloquées, le consommateur fournisse une copie du rapport concernant le vol d'identité ainsi qu'une déclaration selon laquelle les informations ne concernent pas les transactions effectuées par le consommateur. Les lois de la Californie exigent que le consommateur fournisse au bureau, en même temps que la demande, une copie du rapport de police. Au Canada, la déclaration de vol d'identité (que l'on obtient sur le site Web du Comité sur les mesures en matière de consommation, le site Web des provinces ou celui de PhoneBusters), qui doit obligatoirement être assortie d'un rapport de police, pourrait servir de preuve pour établir que l'information découle d'un vol d'identité.

La FACTA et les lois de la Californie donnent aux bureaux de crédit le pouvoir de refuser de bloquer des informations ou d'annuler le blocage si la demande a été produite par erreur, si le consommateur a présenté les faits de façon erronée ou s'il a reçu des biens ou des services grâce à la transaction visée par le blocage. Afin d'atténuer les difficultés auxquelles les victimes font face lorsqu'elles essaient de rétablir leur réputation, les lois californiennes ajoutent que les bureaux de crédit doivent croire les victimes sauf s'ils ont des motifs raisonnables et fondés sur des faits vérifiables de mettre en doute l'authenticité des documents fournis à l'appui de la demande de blocage.

Cette option pourrait prévoir une norme semblable visant à garantir que les bureaux de crédit sont protégés contre les consommateurs qui contournent les règles. On pourrait aussi prévoir un délai de 30 jours pour permettre aux bureaux de crédit de vérifier avec les créanciers la déclaration des consommateurs selon laquelle ils ont été victimes d'un vol d'identité, avant de bloquer l'information. Si l'on veut éviter que les différents bureaux de crédit ne répondent à cette demande chacun à leur façon, on pourrait aussi exiger qu'ils élaborent une approche simplifiée

visant à régler les plaintes qui concernent les rapports de crédit inexacts contenant des informations sur des dettes contractées par des voleurs d'identité. En faisant circuler les informations, on simplifie énormément le processus que doivent suivre les victimes qui essaient de rétablir leur réputation et ont garanti qu'elles ne seront pas traitées de manière différente par différents bureaux de crédit. Donc, si un bureau de crédit supprime les renseignements qui concernent les dettes contractées par un voleur d'identité, il en informera les autres bureaux de crédit, qui devront eux aussi supprimer ces informations du dossier de crédit de la personne visée.

QUESTIONS POUR L'OPTION VIII

1. Pensez-vous que cette option assurerait une meilleure protection contre le vol d'identité? Pourquoi/pourquoi pas?
2. Quels seraient les coûts de cette option? Permettrait-elle des économies compensatoires? Qui devrait assumer les coûts?
3. Devrait-on prévoir des exceptions? Si oui, lesquelles?
4. Faudrait-il que cette disposition soit associée à des pénalités?
5. Pour cette option, qui serait le premier responsable des pertes associées au vol d'identité?
6. Cette option comporte-t-elle des désavantages pour les consommateurs ou l'industrie? Veuillez fournir des détails.
7. Faut-il bloquer les informations dès le moment où le consommateur présente une déclaration de vol d'identité? Doit-on accorder au bureau de crédit un certain délai pour qu'il puisse vérifier les faits auprès du créancier avant de bloquer les informations?
8. Les informations bloquées devraient rester au dossier à des fins d'enquête; à quel moment pourra-t-on les éliminer complètement du dossier?
9. Les procédures de blocage devraient-elles être rationalisées jusqu'au point où des informations bloquées par un bureau de crédit seront bloquées de la même façon dans les autres bureaux de crédit? Alternativement, pourrait-on créer une chambre de compensation centrale qui traitera les demandes des consommateurs voulant que l'on bloque certaines informations concernant les dettes contractées par des voleurs d'identité?

Option IX - Rendre les organismes responsables des préjudices.

Les organismes seraient responsables des préjudices causés par leur défaut de se conformer aux directives suivantes :

A. Les créanciers doivent :

a) communiquer avec les consommateurs à un numéro de téléphone prédéterminé avant d'accorder le crédit, lorsqu'un avertissement de fraude a été versé au dossier de crédit.

B. Les bureaux de crédit doivent :

a) vérifier de façon appropriée l'identité d'une personne qui demande un rapport de crédit;
b) imposer un gel du crédit au dossier de crédit d'un consommateur, conformément aux dispositions de l'option 4;
c) ajouter un avertissement de fraude à un dossier, sur demande, conformément aux dispositions de l'option 6;
d) bloquer des informations conformément aux dispositions de l'option 8.

C. Tous les organismes doivent :

a) tronquer le numéro de carte de paiement, conformément aux dispositions de l'option 1;
b) aviser les personnes touchées par un bris de sécurité conformément aux dispositions de l'option 5.

Tous ces organismes seraient tenus légalement responsables des préjudices subis par les victimes d'un vol d'identité s'ils ne se sont pas conformés à ces dispositions.

Comme on vient de l'expliquer, il n'y a aucune commune mesure, sur les marchés, entre les coûts du vol d'identité et les revenus générés par un accès facile au crédit à la consommation. Cet écart signifie qu'il n'y pas de mesures incitatives suffisantes pour convaincre les bureaux de crédit et les institutions financières de contrôler les fraudes de manière plus dynamique et de corriger les informations erronées. Un droit d'action prévu par la loi constituerait peut être, pour l'industrie, un bon motif d'agir pour cerner les cas de vol d'identité et corriger les informations erronées qui figurent dans les dossiers.

Jusqu'ici, les tribunaux ont hésité à tenir les créanciers et les bureaux de crédit responsables. Selon cette option, les consommateurs auraient le droit d'intenter une action civile; les victimes pourraient donc poursuivre les organismes qui ne prennent pas des mesures raisonnables pour

prévenir le vol d'identité. Cette option serait assortie d'un montant minimum de dommages-intérêts légaux, de la même façon que les lois américaines imposent des sanctions civiles minimales de 500 à 2 500 $ pour infractions aux dispositions sur le gel du crédit ou les avertissements de fraude (voir l'option 6, ci-dessus). Ces pénalités minimales supprimeraient, pour les victimes, l'obligation d'avoir à prouver qu'elles ont subi un préjudice spécifique en leur permettant de recevoir un montant minimal fixé d'avance à titre d'indemnisation pour les souffrances morales et pour le temps qu'elles ont consacré à réparer leur réputation.

Cette option donnerait aussi aux victimes le droit d'obtenir une ordonnance de la cour afin d'interdire à un bureau de crédit de vendre des rapports de crédit contenant des renseignements sur les dettes contractées en leur nom par des voleurs d'identité.

Cette option modifierait en profondeur les responsabilités des organismes qui traitent des renseignements personnels. Elle pourra entraîner une réduction des cas de fraude et des pertes connexes. Elle pourrait aussi, probablement, provoquer une hausse des coûts dans l'industrie du crédit, mais cette hausse serait, toutes proportions gardées, négligeable. L'incertitude que tout cela entraîne pourrait affecter négativement l'industrie du crédit et provoquer une augmentation des coûts du crédit. Mais elle constituerait pour l'industrie du crédit un très bon encouragement à réduire les risques de vol d'identité.

N'oublions pas que les lois fédérales et provinciales sur la protection des renseignements personnels exigent que les organismes protègent les informations qu'ils détiennent contre la divulgation non autorisée. Si les victimes d'un vol d'identité peuvent présentement réclamer des dommages-intérêts pour les préjudices réels subis devant la Cour fédérale ou les tribunaux des provinces, elles doivent s'engager dans un processus difficile, en deux étapes, qui ne prévoit pas d'option simplifiée, par exemple une pénalité minimale, comme on vient de le décrire.

QUESTIONS POUR L'OPTION IX

1. Pensez-vous que cette option assurerait une meilleure protection contre le vol d'identité? Pourquoi/pourquoi pas?
2. Quels seraient les coûts de cette option? Permettrait-elle des économies compensatoires? Qui devrait assumer les coûts?
3. Devrait-on prévoir des exceptions? Si oui, lesquelles?
4. Pour cette option, qui serait le premier responsable des pertes associées au vol d'identité?
5. Cette option comporte-t-elle des désavantages pour les consommateurs ou l'industrie? Veuillez fournir des détails.

Option X – Renseigner les victimes au sujet de leurs droits.

Les organismes doivent garantir un accès facile aux informations concernant les droits des victimes. Réparer les préjudices causés par un vol d'identité est un processus long et coûteux. Les victimes ont besoin d'information en langage clair et simple sur la façon de régler des dettes frauduleuses, de rétablir leurs dossiers de crédit et de corriger leurs données financières.

Selon cette option, les organismes seraient obligés de donner un accès rapide aux informations pour les victimes d'un vol d'identité. Les institutions devraient aussi fournir des renseignements sur les organismes centraux de signalement ou de supervision (p. ex. PhoneBusters), qui peuvent aider les victimes à se rétablir après une fraude.

De plus, les consommateurs devraient pouvoir exercer leurs droits en utilisant les mêmes moyens qu'ils prennent pour obtenir des services – le téléphone, l'Internet, les communications écrites ou en personne.

Selon la FACTA, les bureaux de crédit doivent fournir aux victimes un aperçu de leurs droits. On doit en particulier leur dire qu'elles peuvent obtenir une copie de leurs rapports de crédit et de leurs cotes de crédit et qu'elles peuvent contester les renseignements qui figurent dans le rapport. Selon les lois de la Californie, le sommaire des droits doit aussi fournir un numéro de téléphone sans frais que la victime peut utiliser pour communiquer avec le bureau de crédit. Au Texas, le sommaire des droits fournit des informations sur la façon de demander ou de supprimer un avertissement de fraude ou un gel du crédit.

Selon la LPRPDE et les lois provinciales sur la protection des renseignements personnels, les organismes sont tenus de fournir aux personnes des informations concernant leurs politiques et pratiques en matière de gestion des renseignements personnels. On pourrait modifier ces lois pour indiquer clairement que les institutions financières et les bureaux de crédit sont obligés de fournir ces informations aux consommateurs. Il serait peut-être nécessaire de modifier les lois provinciales/territoriales sur la protection des consommateurs et les renseignements concernant le consommateur, les lois fédérales s'appliquant aux banques et les lois provinciales/territoriales s'appliquant aux coopératives d'épargne et de crédit.

QUESTIONS POUR L'OPTION X

1. Pensez-vous que cette option assurerait une meilleure protection contre le vol d'identité?
2. Quels seraient les coûts de cette option? Permettrait-elle des économies compensatoires? Qui devrait assumer les coûts?
3. Devrait-on prévoir des exceptions? Si oui, lesquelles?
4. Faudrait-il que cette disposition soit associée à des pénalités?
5. Pour cette option, qui serait le premier responsable des pertes associées au vol d'identité?
6. Cette option comporte-t-elle des désavantages pour les consommateurs ou l'industrie? Veuillez fournir des détails.

7. Les organismes doivent-ils se doter d'un numéro sans frais à cette fin?
8. Quel type d'information devraient-ils fournir – renseignements sur le processus de règlement des différends, sur la prévention des vols d'identité (avertissements, gels, blocage de renseignements), la déclaration de vol d'identité, les noms et numéros de téléphone de personnes-ressources, etc.?
9. Faudrait-il créer un organisme centralisé distinct à cette fin? Cet organisme devrait-il aussi faciliter la présentation de demandes d'avertissements de fraude après un bris de sécurité, le gel du crédit ou le blocage de renseignements erronés en élaborant un processus simplifié?

Conclusion

Le vol d'identité est un problème en croissance au Canada. Les voleurs d'identité se sont rapidement adaptés aux nouvelles technologies, et les lois canadiennes n'ont pas été mises à jour assez rapidement. Les options que l'on vient de présenter visent à renforcer les lois existantes dans le but de compliquer la tâche des voleurs d'identité qui veulent s'approprier de façon frauduleuse des renseignements personnels et à permettre aux victimes de découvrir plus rapidement qu'il y a eu fraude et de s'en rétablir.

L'application de certaines des propositions du présent document exigera des ressources appropriées; on pense à la troncation des numéros de carte de paiement, aux interdictions visant l'utilisation du NAS et à l'élimination des renseignements erronés sur le crédit qui découlent de l'action d'un voleur d'identité. D'autres propositions, par exemple, de devoir aviser les personnes touchées par un bris de sécurité, l'ajout d'avertissements de fraude et la vérification obligatoire des personnes qui demandent un rapport de crédit ou qui veulent obtenir du crédit constituent en fait une simple norme que les organismes devront respecter de façon à ne pas être tenus responsables de préjudices ultérieurement.

En participant à des mesures coordonnées, tous les intervenants concernés – les consommateurs, les entreprises, les institutions financières, les bureaux de crédit et les gouvernements – garantissent qu'ensemble nous pouvons régler ce coûteux problème.

Nous attendons avec intérêt vos commentaires sur l'un ou l'autre des enjeux dont il a été question dans ce document. Si vous avez des questions, n'hésitez pas à les communiquer par courriel à : info@cmcweb.ca , et inscrire « Question – vol d'identité » dans le champ destiné au sujet.

[1] Un bureau de crédit, ou une agence d'évaluation du crédit, recueille et vend des informations concernant la solvabilité d'une personne. Les créanciers potentiels achètent le rapport de crédit

afin d'évaluer le niveau de risque d'une personne avant de lui accorder un crédit.

[2] *Concern about Identity Theft Growing in Canada*, Ipsos Reid, (28 février 2003).

[3] Philippa Lawson, John Lawford, *Identity Theft: The Need for Better Consumer Protection*, Centre pour la défense de l'intérêt public, octobre 2003. Le document cite diverses sources, notamment : California Public Interest Research Group (CALPIRG), *Nowhere to Turn: Victims Speak Out on Identity Theft*, 1er mai 2000, (http://www.calpirg.org/consumer/privacy/idtheft2000.pdf); Commission fédérale du commerce, *Identity Theft Survey Report*, septembre 2003, (http://www.ftc.gov/os/2003/09/synovate report.pdf) (rapport Synovate).

[4] *R. v. Stewart* (1988), 63 C.R. (3d) 305, 41 C.C.C. (3d) 481 (C.S.C.).

[5] *Op. cit.*, note 3. Le nombre total dépasse 100 % : c'est que les personnes qui signalent un vol d'identité sont victimes à plus d'un titre. Autrement dit, des voleurs d'identité utilisent les renseignements personnels qui concernent une personne pour obtenir une carte de crédit, un prêt, etc.

[6] Groupe de travail binational sur les fraudes transfrontalières par marketing de masse, *Rapport du procureur général des États-Unis et du Solliciteur général du Canada*, mai 2003, (http://www.psepc-sppcc.gc.ca/publications/policing/Mass_Marketing_Fraud_f.asp).

[7] Au Canada, le sondage a été réalisé par Environics, et aux États-Unis, par la Commission fédérale du commerce.

[8] Consulter l'Association des banquiers canadiens, (http://www.cba.ca/fr/content/reports/Identity%20Theft%20-%20A%20Prevention%20Policy%20is%20Needed%20FRE.pdf).

[9] Collins, J.M. et Hoffman, S.K., « Identity Theft: Predator Profiles », *Security Journal*. On peut obtenir le manuscrit en s'adressant à Judith Collins à l'adresse suivante : judithc@msu.edu.

[10] "Vulnerability of computer info revealed," Daily Herald (Moose Jaw), February 5, 2003, p. 4.

[11] Mark Hume, *Globe and Mail*, March 16, 2004.

[12] Matt Hines, Cnet news.com, February 18, 2005

[13] Jeff Sovern, "Stopping Identity Theft," *Journal of Consumer Affairs*, vol. 38, no. 2, Winter 2004, p. 237.

[14] Association des banquiers canadiens

http://www.cba.ca/fr/content/stats/050210-Credit%20cards-FR.pdf.

[15] Jeff Sovern, *supra*, note 13, p. 238.

[16] Encore une fois, il n'existe pas de statistiques canadiennes sur le temps consacré. Aux États-Unis, Synovate, *op. cit.*, note 9, indique que les victimes consacrent de 30 à 60 heures à réparer les préjudices qui découlent d'un vol d'identité, et la Privacy Rights Clearinghouse, de son côté, évalue qu'elles y consacrent 175 heures (Beth Givens, *Identity Theft: How It Happens, Its Impact on Victims, and Legislative Solutions*, 12 juillet 2000, témoignage écrit prononcé devant le Senate Judiciary Subcommittee on Technology, Terrorism, and Government Information des Etats-Unis).

[17] Lawson et Lawford, *op. cit.*, note 3.

[18] Aux États-Unis, des victimes d'un vol d'identité ont été arrêtées pour un crime commis par une personne qui utilisait les renseignements personnels les concernant.

[19] Autrement dit, ces organismes doivent vérifier qu'une personne est vraiment la personne qu'elle prétend être avant de faire affaire avec elle par voie électronique.

[20] Voir aussi le *Code canadien de pratiques pour la protection des consommateurs dans le commerce électronique* élaboré par le gouvernement fédéral à partir des *Principes d'authentification électronique*. On peut consulter le *Code* à l'adresse suivante : www.cmcweb.ca/commerceelectronique

[21] En vertu des lois constitutionnelles des États-Unis, certaines dispositions de la FACTA ont préséance sur les lois des différents États qui traitent des mêmes questions.

[22] Industrie Canada, *Principes d'authentification électronique – Cadre canadien*, 10 mai 2004, (http://e-com.ic.gc.ca/epic/internet/inecic-ceac.nsf/fr/h_gv00240f.html).

[23] Mastercard indique que 35 % des pertes subies au Canada par l'entreprise en raison de fraude sur carte de crédit sont dues au vol d'identité; à titre de comparaison, ce pourcentage s'établit à seulement 7 % à l'échelle mondiale. Selon certains analystes, cet écart vient du fait que les numéros d'assurance sociale sont utilisés de façon très généralisée au Canada à des fins d'identification dans les activités commerciales. En Europe, les cartes d'identité sont en général utilisées uniquement pour la vérification en personne de l'identité, et ne peuvent donc soutenir le vol d'identité (Sullivan, *op. cit.*, note 8).

[24] Rapport du Bureau du vérificateur général du Canada, 2002 : Développement des ressources humaines Canada - L'intégrité du numéro d'assurance sociale.