Commissariat
à la protection de la
vie privée du Canada

VÉRIFICATION DE
CERTAINS COURTIERS EN PRÊTS HYPOTHÉCAIRES

Article 18 de la *Loi sur la protection des renseignements personnels et les documents électroniques*

RAPPORT FINAL

2010

Commissariat à la protection de la vie privée du Canada
112, rue Kent
Ottawa (Ontario) K1A 1H3

613-947-1698, 1-800-282-1376
Télécopieur : 613-947-6850
ATS : 613-992-9190
Suivez-nous sur Twitter : @privacyprivee

No de catalogue IP54-32/2010
ISBN 978-1-100-51559-5
Cette publication se trouve également sur notre site Web au **www.priv.gc.ca**.

Table des matières

Points principaux

ÉLÉMENTS EXAMINÉS

Entre juillet et décembre 2008, 14 courtiers en prêts hypothécaires ont signalé au Commissariat à la protection de la vie privée de nombreuses atteintes à la protection des renseignements personnels touchant des centaines de personnes. L'atteinte à la protection des renseignements personnels se définit comme la perte, la consultation ou la communication non autorisées de renseignements personnels qui se produisent lorsque les mécanismes de sécurité d'une organisation sont mis en échec. Comme les atteintes signalées se sont toutes produites en Ontario, nous avons fait une vérification de cinq courtiers en prêts hypothécaires établis dans cette province. Ils ont été choisis en fonction du nombre de personnes touchées, de l'occurrence de multiples atteintes et de la nature de celles-ci.

Nous avons examiné les politiques et procédures en matière de protection de la vie privée qui sont en place ainsi que les formulaires de demande de prêt hypothécaire utilisés. Nous avons procédé à une inspection matérielle des bureaux des courtiers en prêts hypothécaires et évalué les mesures en place pour sécuriser les locaux des courtiers. Nous avons examiné les systèmes de technologie de l'information de même que les mesures de contrôle entourant la façon dont les courtiers en prêts hypothécaires ont accès aux rapports de solvabilité des agences d'évaluation du crédit.

IMPORTANCE DE L'EXAMEN

Les courtiers en prêts hypothécaires représentent un segment de plus en plus important du secteur des prêts hypothécaires au Canada. Les courtiers et leurs agents obtiennent, utilisent et communiquent régulièrement des renseignements personnels dans le cadre de leur travail. Pour évaluer la solvabilité des clients et la pertinence des produits hypothécaires, le secteur des prêts hypothécaires utilise les rapports de solvabilité des agences d'évaluation du crédit au moyen d'un outil Web.

Deux points communs se sont dégagés dans les atteintes signalées au Commissariat. D'abord, une personne, se faisant passer pour un agent en hypothèques autorisé, a réussi à obtenir un emploi dans chacune des entreprises de courtage hypothécaire que nous avons vérifiées. Deuxièmement, l'agent frauduleux a utilisé l'outil Web donnant accès aux rapports de solvabilité et a obtenu des centaines de rapports n'ayant rien à voir avec les demandes de prêt hypothécaire.

CONSTATATIONS

Nous avons constaté que les courtiers ont resserré considérablement leurs processus d'embauche à la suite de ces atteintes. De plus, ils les ont signalées au Commissariat de façon proactive. Nous avons cependant constaté que les courtiers en prêts hypothécaires étaient incapables de démontrer que

des mécanismes de sécurité adéquats étaient en place pour protéger les renseignements personnels relevant d'eux. Les documents, notamment les dossiers de demande de prêt hypothécaire, les rapports de solvabilité et d'autres documents sensibles, n'étaient pas toujours conservés en lieu sûr. Nous avons également noté que les courtiers ne disposaient pas toujours de systèmes et d'outils adéquats pour s'assurer que personne n'avait accès sans autorisation aux rapports de solvabilité.

Bien que la plupart des courtiers soumis à une vérification avaient des politiques sur la protection de la vie privée, ces dernières n'étaient pas toujours assez détaillées pour indiquer clairement les pratiques en matière de traitement de l'information ou comment elles permettaient de respecter les obligations imposées par la *Loi sur la protection des renseignements personnels et les documents électroniques* (LPRPDE), et ces politiques n'étaient pas toujours rendues accessibles aux clients. Nous avons constaté qu'on ne demandait pas toujours aux clients leur consentement avant d'obtenir un rapport de solvabilité et que certains courtiers utilisaient les renseignements concernant un client à d'autres fins que celles pour lesquelles ils avaient été recueillis.

Nous avons constaté que les courtiers en prêts hypothécaires n'éliminaient pas toujours les demandes de prêts hypothécaires non approuvées en temps opportun et de façon sécuritaire. Par ailleurs, notre vérification a révélé que les courtiers en prêts hypothécaires et leurs agents n'étaient pas pleinement conscients de leur rôle dans la protection des renseignements personnels relevant d'eux et qu'ils n'avaient pas reçu une formation adéquate sur leurs responsabilités à ce chapitre. En raison de l'absence de politiques et de procédures détaillées sur la protection de la vie privée, et d'une indication claire quant à la responsabilité de leur mise en œuvre, aucun des courtiers vérifiés ne s'acquittait pleinement des obligations que lui impose la LPRPDE pour que les renseignements personnels de ses clients et d'autres personnes soient protégés.

Sur les cinq courtiers que nous avons vérifiés, les quatre qui étaient toujours en activité ont répondu à nos recommandations et les ont toutes acceptées. Leurs réponses figurent à l'annexe A.

Introduction

LES COURTIERS EN PRÊTS HYPOTHÉCAIRES

1. Les courtiers en prêts hypothécaires représentent un segment de plus en plus important du secteur des prêts hypothécaires au Canada. Une enquête commandée par la Société canadienne d'hypothèques et de logement a révélé qu'en 2009 les courtiers en prêts hypothécaires s'étaient chargés de 25 % de toutes les transactions hypothécaires et de 44 % des transactions effectuées par les clients qui achetaient leur première maison. Les courtiers et leurs agents offrent des produits, des taux et des conditions aux personnes qui cherchent à obtenir un prêt hypothécaire, et ils servent d'intermédiaires entre ces personnes et les prêteurs, y compris les banques et les coopératives de crédit.

2. Les entreprises de courtage hypothécaire peuvent être des franchises affiliées à un bureau principal tout en continuant d'être détenues et de fonctionner de façon indépendante. Ces entreprises emploient du personnel qui travaille dans les locaux de l'entreprise ou à domicile. Elles peuvent aussi être indépendantes, sans affiliation aucune avec une autre entreprise. Pour les besoins de la vérification, le terme « courtier en prêts hypothécaires » désigne le franchisé ou le courtier principal. Les courtiers en prêts hypothécaires sont assujettis aux lois de la province dans laquelle ils exercent leurs activités. En Ontario, les courtiers et les agents sont autorisés à accorder des prêts hypothécaires. La *Loi de 2006 sur les maisons de courtage d'hypothèques, les prêteurs hypothécaires et les administrateurs d'hypothèques* interdit aux agents de négocier des hypothèques, à moins de le faire sous la supervision d'un courtier. De plus, comme ces courtiers en prêts hypothécaires établis en Ontario recueillent, utilisent et communiquent des renseignements personnels dans le cadre de leurs activités commerciales, ils sont assujettis à la *Loi sur la protection des renseignements personnels et les documents électroniques* (LPRPDE).

3. Les courtiers et les agents recueillent des renseignements personnels dans le cadre des demandes de prêt hypothécaire. Ces renseignements peuvent comprendre le nom, l'adresse, le numéro de téléphone, la date de naissance, le numéro d'assurance sociale (NAS), l'état matrimonial, les personnes à charge, l'emploi, le revenu, les actifs et les dettes. Pour déterminer l'admissibilité d'une personne à un prêt hypothécaire, les courtiers et agents consultent la base de données d'une agence d'évaluation du crédit par l'entremise d'un outil Web mis à leur disposition par un tiers. Cet outil leur permet de gérer tout le processus de demande de prêt hypothécaire, d'obtenir des rapports de solvabilité, d'envoyer les demandes aux prêteurs et d'obtenir un financement hypothécaire.

DES CENTAINES DE RAPPORTS DE SOLVABILITÉ ONT ÉTÉ CONSULTÉS SANS AUTORISATION

4. Entre juillet et décembre 2008, 14 courtiers en prêts hypothécaires de l'Ontario ont signalé au Commissariat à la protection de la vie privée (CPVP) de nombreuses atteintes à la protection des renseignements personnels touchant des centaines de personnes. Dans tous les cas, une personne se faisant passer pour un agent en hypothèques expérimenté avait téléchargé des rapports de solvabilité, en utilisant l'outil Web

d'un tiers, pour son propre usage. Ces atteintes font actuellement l'objet d'une enquête policière.

5. Les courtiers ont découvert le vol présumé des rapports de solvabilité de l'une de ces trois façons :
   - après avoir été alerté par une personne qui avait consulté son rapport de solvabilité;
   - après avoir reçu une facture anormalement élevée pour des rapports de solvabilité;
   - après avoir été contactés par des agences d'évaluation du crédit qui voulaient signaler des activités suspectes.
6. Les rapports de solvabilité contiennent une grande quantité de renseignements personnels. Ils sont intéressants pour les criminels car ils peuvent leur servir à commettre des vols d'identité ou des fraudes d'identité.
7. Aux termes de l'article 18 de la LPRPDE, la commissaire à la protection de la vie privée du Canada est habilitée à procéder à la vérification d'une organisation si elle a des motifs raisonnables de croire que l'organisation a contrevenu à la *Loi*. Par conséquent, la commissaire à la protection de la vie privée a évalué les faits entourant les atteintes à la protection des renseignements personnels et déterminé qu'il y avait des motifs raisonnables pour entreprendre une vérification des pratiques de certains courtiers en matière de gestion des renseignements personnels.

OBJET DE LA VÉRIFICATION

8. Étant donné que les atteintes à la protection des renseignements personnels se sont toutes produites en Ontario, cinq courtiers en prêts hypothécaires établis dans cette province ont été soumis à une vérification. Ils ont été choisis en fonction du nombre de personnes touchées, de l'occurrence de multiples atteintes et de la nature de celles-ci. La vérification avait pour objectif de déterminer si les courtiers en prêts hypothécaires ontariens choisis avaient élaboré et mis en œuvre des politiques et procédures pour protéger les renseignements personnels de leurs clients et d'autres personnes. On trouvera dans la section **Au sujet de la vérification** du présent rapport des informations sur la portée de la vérification ainsi que les critères et la méthode utilisés.
9. La vérification ne porte pas sur la gestion des renseignements personnels des courtiers et des agents en prêts hypothécaires ou des employés. Elle porte sur les renseignements liés aux consommateurs, aux clients et à d'autres personnes. Les agences d'évaluation du crédit n'ont pas été examinées dans le cadre de cette vérification. Comme l'alinéa 18(1)*d*) de la LPRPDE nous interdit de mener des activités de vérification dans une maison d'habitation, nous n'avons pu évaluer les activités des agents qui travaillent à domicile. Enfin, nous n'avons pas soumis à une vérification le tiers qui fournissait l'outil Web donnant accès aux rapports de solvabilité.

Les rapports de solvabilité peuvent contenir les renseignements suivants :

- nom, adresse, date de naissance et possiblement numéro d'assurance sociale;
- liste des organismes qui ont demandé une copie du dossier de crédit au cours d'une période de temps précise;
- renseignements sur les prêts obtenus, les faillites et les jugements;
- dettes antérieures et actuelles, y compris celles dont le paiement a été confié à une agence de recouvrement;
- historique des transactions et des paiements de crédit.

Observations et recommandations

PROTECTION DES RENSEIGNEMENTS PERSONNELS

10. L'une des principales raisons expliquant pourquoi les atteintes se sont produites chez les courtiers en prêts hypothécaires que nous avons vérifiés, c'est que les systèmes et les mesures de contrôle visant à empêcher l'accès inopportun aux rapports de solvabilité étaient insuffisants. Les organisations assujetties à la LPRPDE doivent protéger les renseignements personnels dont elles sont responsables en mettant en place des mesures de sécurité qui sont proportionnelles à leur degré de sensibilité. Par conséquent, les courtiers en prêts hypothécaires doivent mettre en place des mesures de contrôle matérielles, techniques et administratives suffisantes pour protéger les renseignements personnels de leurs clients et d'autres personnes.

11. Nous avons examiné les politiques et les procédures, les ententes, les documents sur le déroulement des processus et les systèmes de TI. Nous nous sommes rendus sur place pour examiner les bureaux des courtiers en prêts hypothécaires. Nous avons aussi mis à l'épreuve les mesures de contrôle entourant l'accès des courtiers aux rapports de solvabilité des agences d'évaluation du crédit, obtenus par le biais d'un outil Web fourni par un tiers.

Sécurité physique variable d'une agence de courtage à l'autre

12. Compte tenu de la sensibilité de l'information personnelle et financière utilisée, nous avons cherché à savoir si les courtiers en prêts hypothécaires avaient déterminé les menaces, établi les risques connexes et recommandé des mesures d'atténuation pour corriger les lacunes constatées. Aucun des courtiers vérifiés n'avait entrepris ces actions, que l'on appelle aussi collectivement une « évaluation de la menace et des risques ».

13. Une évaluation de la menace et des risques sert à déceler les lacunes dans les processus et les systèmes et à les atténuer. Ce type d'évaluation aiderait les courtiers en prêts hypothécaires à déterminer le niveau de sécurité minimum acceptable requis pour protéger l'information. Nous avons constaté que le niveau de sécurité des cinq courtiers vérifiés était variable. Par exemple :

    - Certains courtiers en prêts hypothécaires n'avaient pas de système d'alarme pour protéger leurs locaux. L'un de ceux qui n'en avait pas nous a informés qu'un commerce adjacent avait été cambriolé;
    - La majorité des courtiers que nous avons examinés avaient des murs robustes et sûrs, allant du sol jusqu'au plancher supérieur autour du périmètre des bureaux, mais l'un d'eux n'en avait pas;
    - Aucun d'entre eux n'avait de murs intérieurs solides. Les murs intérieurs de tous les courtiers n'allaient que du plancher au plafond, ce qui les exposait au risque d'un accès non autorisé à partir des bureaux voisins par l'intermédiaire du vide sanitaire entre le plafond et l'étage supérieur.

14. Une telle évaluation et la prise de mesures donnant suite aux recommandations aideraient les courtiers à respecter les obligations en matière de sécurité qu'impose la LPRPDE. En l'absence d'une évaluation de la menace et des risques, les courtiers soumis à une vérification n'ont pas pu démontrer qu'ils avaient cerné les risques associés à la sécurité et pris les mesures d'atténuation qui s'imposaient.

Lacunes dans l'entreposage de documents

15. Selon les Principes généralement reconnus en matière de protection des renseignements personnels de l'Institut canadien des comptables agréés, les mesures de protection physique peuvent comprendre l'utilisation de classeurs verrouillés, les systèmes de contrôle des accès par carte, les clés physiques, les fichiers des entrées avec signature, et d'autres techniques permettant de contrôler l'accès aux bureaux, aux centres de données ainsi qu'à d'autres lieux où des renseignements personnels sont traités ou stockés.

16. Comme il a été mentionné auparavant, les demandes de prêt hypothécaire contiennent des renseignements personnels de nature sensible qui doivent être conservés de manière sécuritaire. Nous avons constaté différentes pratiques de conservation parmi les courtiers. Par exemple, une partie des courtiers que nous avons examinés utilisaient des classeurs sécurisés, alors que d'autres conservaient leurs dossiers dans des classeurs déverrouillés ou les empilaient sur le plancher ou sur des bureaux accessibles à tous. Nous avons aussi constaté qu'un courtier entreposait son surplus de dossiers dans le stationnement non sécurisé de l'édifice où se trouvaient ses bureaux, ce qui aurait pu donner lieu à une atteinte à la protection des renseignements personnels. Nous avons remarqué qu'un autre courtier s'était organisé pour que tous les dossiers de demandes de prêt hypothécaire inactifs ou fermés soient entreposés chez un tiers offrant des services d'archivage de documents accrédité par la *National Association for Information Destruction*.

17. Au cours des entrevues avec le personnel au sujet des mesures de sécurité, nous avons été informés que les demandes de prêt hypothécaire pouvaient être conservées au domicile du courtier, et que les agents pouvaient aussi conserver chez eux des copies des demandes non approuvées. La sécurité des dossiers se trouvant à l'extérieur des bureaux n'a pu être vérifiée puisque certains courtiers et agents conservaient des copies des dossiers à leur domicile et que l'examen de ceux-ci échappe à la portée de la vérification.

18. En plus des dossiers papier, tous les courtiers examinés conservaient des dossiers électroniques, notamment des demandes de prêt hypothécaire, des rapports de solvabilité et des feuilles de calcul. Les réseaux informatiques que nous avons examinés étaient protégés par des mots de passe et des logiciels antivirus; toutefois, aucun de ces réseaux n'avait été mis à l'épreuve pour déceler la présence de vulnérabilités et s'assurer que des mesures de protection adéquates étaient en place.

Contrôle inadéquat de l'accès aux rapports de solvabilité

19. Les courtiers et agents en hypothèques utilisent un outil Web pour obtenir des rapports de solvabilité afin d'évaluer la solvabilité des clients qui souhaitent se procurer des produits hypothécaires. Les atteintes à la protection des renseignements personnels signalées au CPVP se sont produites lorsque des agents ont téléchargé des centaines de rapports de solvabilité qui n'étaient pas nécessaires à des fins hypothécaires. Les atteintes en question ont été commises des personnes qui se faisaient passer pour des agents en prêts hypothécaires et qui téléchargeaient une quantité de rapports de solvabilité dépassant largement la norme. Cette activité est passée inaperçue pendant un certain temps. Si les courtiers en prêts hypothécaires avaient mis en place des mesures de contrôle appropriées pour prévenir l'utilisation non autorisée de l'outil Web, ils auraient pu atténuer le risque d'accès abusif aux rapports de solvabilité.

20. En testant l'outil Web, nous avons constaté que des mesures étaient en place pour limiter l'accès au système de production de rapports de solvabilité. Le système était chiffré et nécessitait un mot de passe pour ouvrir une session, mais il était impossible pour les courtiers d'exercer une surveillance proactive et d'être alertés quand des activités suspectes se produisaient, ou d'établir des limites quant au nombre de rapports de solvabilité pouvant être téléchargés.

21. Ces types de contrôles sont utilisés par plusieurs organisations, notamment celles qui offrent à leurs employés des cartes de crédit professionnelles. Ils leur permettent de surveiller les achats, de limiter les dépenses et d'en faire le suivi à l'aide de rapports personnalisés, ce qui permet de réduire les possibilités de fraude.

22. Actuellement, la seule manière pour les courtiers en prêts hypothécaires de savoir si quelqu'un a accédé de manière abusive au système de production des rapports de solvabilité, c'est de consulter le fichier journal de l'ordinateur, qui enregistre l'information sur les rapports de solvabilité auxquels a eu accès un utilisateur précis. Cependant, l'examen du fichier journal est une mesure a posteriori. En outre, les courtiers sont incapables de limiter le nombre de rapports de solvabilité qui peuvent être téléchargés.

23. Pendant nos vérifications, nous avons aussi constaté que, lorsqu'un rapport de solvabilité était consulté, une copie de ce rapport était conservée dans le dossier « temporaire » de l'ordinateur du demandeur. Si le contenu de ce dossier n'était pas supprimé, le rapport de solvabilité demeurait dans l'ordinateur.

24. Même si on ne nous a pas informés que cette vulnérabilité avait donné lieu à une atteinte à la protection des renseignements personnels, cette situation pourrait représenter un risque grave si les ordinateurs sont partagés ou si les rapports de solvabilité sont consultés sur des ordinateurs publics (p. ex. dans un cybercafé ou une bibliothèque publique), ou si les agents utilisent des ordinateurs domestiques partagés pour consulter les rapports de solvabilité.

25. De plus, quand on se serait débarrassé de ces ordinateurs, à moins que les disques durs aient été effacés comme il se doit, le rapport de solvabilité demeurerait intact et toute personne qui acquerrait l'ordinateur ou le disque dur pourrait y avoir accès.

26. RECOMMANDATION

Les courtiers en prêts hypothécaires vérifiés devraient protéger les renseignements personnels dont ils sont responsables en mettant en place des mesures de sécurité correspondant à leur degré de sensibilité. Il peut s'agir de s'assurer, sans s'y limiter, que :

- des mesures de sécurité physique adéquates sont en place, comme des alarmes et des classeurs pouvant être verrouillés;
- des mesures supplémentaires sont prises pour protéger les rapports de solvabilité et limiter le nombre de rapports pouvant être téléchargés.

DÉTERMINATION DES FINS, COLLECTE, CONSENTEMENT, UTILISATION, CONSERVATION ET COMMUNICATION

27. Les organisations assujetties à la LPRPDE doivent respecter les principes énoncés à l'annexe 1 de la LPRPDE concernant la collecte, l'utilisation et la communication des renseignements personnels. Les courtiers en prêts hypothécaires doivent :

    - déterminer clairement les fins auxquelles les renseignements personnels sont recueillis avant la collecte ou au moment de celle-ci;
    - obtenir le consentement de la personne concernée pour la collecte, l'utilisation et la communication de renseignements personnels;
    - limiter la collecte aux renseignements nécessaires aux fins déterminées;
    - utiliser et communiquer des renseignements personnels uniquement aux fins auxquelles ils ont été recueillis;
    - ne conserver les renseignements personnels qu'aussi longtemps que nécessaire.

28. Pour déterminer dans quelle mesure les courtiers en prêts hypothécaires s'acquittaient de ces obligations, nous avons examiné les politiques en matière de protection de la vie privée pour vérifier si elles tenaient compte des principes pertinents de l'annexe 1 de la LPRPDE. Nous voulions savoir si elles indiquaient clairement le type de renseignements personnels recueillis, comment ils seraient utilisés (y compris comment ils seraient protégés), avec qui ils seraient partagés, quand ils seraient éliminés et qui serait responsable de s'assurer que la politique sur la protection de la vie privée du courtier serait respectée. Nous nous sommes entretenus avec les courtiers en prêts hypothécaires et nous nous sommes rendus dans leurs bureaux. Nous avons également pris connaissance des dispositions sur la protection des renseignements personnels contenues dans les demandes de prêt hypothécaire et les ententes de consentement. Enfin, nous avons examiné les procédures en place pour savoir comment les politiques sur la protection de la vie privée étaient appliquées.

Les politiques sur la protection de la vie privée n'étaient pas toujours assez détaillées

29. Les organisations assujetties à la *Loi* sont tenues de mettre en œuvre des politiques et des pratiques fondées sur les 10 principes énumérés à l'annexe 1 de la LPRPDE. Deux des sièges sociaux que nous avons examinés possédaient des politiques sur la protection de la vie privée très détaillées et les avaient affichées sur leurs sites Web. Ces politiques abordaient les 10 principes relatifs à la protection des renseignements personnels, traitaient de la gestion de l'information de manière assez détaillée et donnaient les coordonnées du responsable de la protection de la vie privée, à qui les questions pouvaient être adressées.

30. Par contre, dans le cas d'un autre courtier, sa politique sur la protection de la vie privée était affichée sur son site Web, mais elle n'expliquait pas assez en profondeur la façon dont il gérait les renseignements personnels. Par exemple, il n'était pas fait mention des 10 principes ni de la façon dont les renseignements personnels des clients seraient utilisés. Bien que la politique ait déclaré que l'organisation s'engageait à assurer la confidentialité des renseignements personnels, aucun détail n'était fourni. Pendant notre vérification, nous avons en outre constaté que le lien menant à la politique sur la protection de la vie privée qui se trouvait sur la page des conditions de service du courtier ne fonctionnait pas.

31. Seulement deux des courtiers examinés avaient inclus dans leurs manuels des politiques et des procédures une politique officielle tenant compte des 10 principes liés à la protection de la vie

privée; cependant, cette politique n'était pas affichée sur le site Web des courtiers et les clients n'y avaient pas accès. Tous les courtiers examinés utilisaient soit un formulaire de consentement du client en matière de protection de la vie privée, soit un formulaire d'accord de confidentialité, que leurs clients devaient signer et par lequel ils consentaient à ce qu'on utilise leurs renseignements personnels. Dans le cas des trois courtiers qui n'avaient pas de politique officielle en matière de protection de la vie privée, la seule référence à la confidentialité et à la protection des renseignements personnels apparaissait dans le formulaire de consentement du client en matière de protection de la vie privée ou dans le formulaire d'accord de confidentialité. Ces formulaires n'étaient cependant pas suffisamment détaillés pour expliquer clairement les pratiques des courtiers au chapitre de la gestion de l'information ou la façon dont ils s'acquittent des obligations que leur impose la *Loi*. En outre, quand nous avons examiné les dossiers des entreprises en question, nous avons constaté que les courtiers n'utilisaient pas systématiquement ces formulaires.

Les fins de la collecte étaient clairement indiquées mais les renseignements recueillis n'étaient pas tous nécessaires dans le cadre d'une demande de prêt hypothécaire

32. Pour s'acquitter des obligations que leur impose la *Loi de 2006 sur les maisons de courtage d'hypothèques*, *les prêteurs hypothécaires et les administrateurs d'hypothèques* en matière d'identification des clients, les courtiers et les agents en prêts hypothécaires de l'Ontario doivent recueillir des renseignements personnels. Les courtiers demandent à leurs clients de remplir un formulaire de demande de prêt hypothécaire qui indique que l'information recueillie servira à obtenir un rapport de solvabilité et un prêt hypothécaire.

33. Nous avons constaté que l'information recueillie par les courtiers pour vérifier l'identité d'un client potentiel pouvait comprendre le numéro de permis de conduire, les renseignements figurant sur l'acte de naissance et le numéro d'assurance sociale (NAS). Les courtiers en prêts hypothécaires utilisaient d'autres documents pour évaluer la situation financière d'un client potentiel, entre autres les feuillets T4 de l'Agence du revenu du Canada et les relevés bancaires. Les établissements de crédit stipulent quels documents les courtiers doivent demander aux clients avant de financer une hypothèque.

34. Les formulaires de demande de prêt hypothécaire n'indiquaient pas que le NAS est facultatif. Nous avons constaté que tous les courtiers et agents en prêts hypothécaires demandaient systématiquement le NAS sur les formulaires de demande et qu'il leur servait souvent à différencier les clients ayant un nom similaire. Toutefois, ce numéro n'est pas nécessaire pour vérifier la solvabilité d'une personne, et la loi n'exige pas qu'il soit recueilli à cette fin. Nous sommes d'avis que le NAS ne devrait pas servir de moyen d'identification général et que les organisations devraient limiter sa collecte, son utilisation et sa communication aux fins prévues par la loi.

Le consentement n'était pas toujours obtenu avant la collecte des renseignements personnels

35. La LPRPDE exige qu'une personne soit informée de toute collecte, utilisation ou communication de renseignements personnels qui la concernent et y consentir. La LPRPDE stipule que, pour que le consentement soit valable, les fins auxquelles les renseignements personnels seront recueillis, utilisés et communiqués doivent être clairement énoncées. La forme du consentement peut varier, mais la LPRPDE exige que l'on obtienne un consentement explicite quand les renseignements sont de nature sensible.

36. Les courtiers en prêts hypothécaires ne devraient recueillir que les renseignements nécessaires et demander le consentement explicite de leur client avant d'obtenir son rapport de solvabilité et de fournir des renseignements personnels à des prêteurs éventuels. Nous avons constaté que même si les courtiers demandaient à leurs clients de consentir par écrit à ce qu'ils aient accès à leurs rapports de solvabilité, dans les cas où les transactions ne se déroulaient pas face à face, les agents obtenaient un consentement verbal puis demandaient aux clients de donner leur consentement par écrit après coup. Cependant, nous avons vu des cas où les rapports de solvabilité avaient été produits avant l'obtention du consentement, et d'autres où aucun document ne permettait d'attester qu'un consentement avait été obtenu.

Les clients ne pouvaient pas refuser l'utilisation secondaire de leurs renseignements personnels

37. Pour obtenir une hypothèque pour leurs clients, les courtiers et les agents en prêts hypothécaires doivent communiquer les renseignements personnels qui les concernent aux agences d'évaluation du crédit et aux prêteurs. Toute autre utilisation de ces renseignements (à des fins de marketing par exemple) devrait être clairement énoncée dans les formulaires de demande de prêt hypothécaire et de consentement. Conformément à la LPRPDE, les courtiers en prêts hypothécaires devraient obtenir le consentement explicite des personnes concernées lorsqu'ils utilisent des renseignements personnels à des fins de marketing.

38. Nous avons examiné les formulaires de consentement de tous les courtiers, et nous avons constaté qu'ils indiquaient que les renseignements personnels recueillis pouvaient servir à des fins de marketing et d'autres utilisations secondaires. Trois des courtiers que nous avons vérifiés nous ont informés que certains renseignements personnels (nom et numéro de téléphone) pouvaient être communiqués à des agents immobiliers, des planificateurs financiers et d'autres fournisseurs de services sous la forme de listes d'acheteurs potentiels. Nous avons également constaté que les formulaires de consentement de tous les courtiers vérifiés leur permettaient d'utiliser les renseignements personnels recueillis à des fins de marketing comme l'envoi de bulletins et de cartes d'anniversaire aux clients. Les formulaires de consentement examinés n'offraient pas aux clients un choix clair leur permettant de refuser les utilisations secondaires de leurs renseignements personnels.

Les dossiers de prêts hypothécaires refusés ne devraient pas être conservés plus longtemps que nécessaire

39. La *Loi de 2006 sur les maisons de courtage d'hypothèques, les prêteurs hypothécaires et les administrateurs d'hypothèques* oblige les courtiers en prêts hypothécaires à conserver tous les documents liés à une demande de prêt hypothécaire pendant au moins six ans après l'échéance du prêt hypothécaire. Comme cette obligation est entrée en vigueur en 2006, les courtiers que nous avons examinés n'avaient pas de dossiers qui satisfaisaient à cette exigence.

40. Nous avons cependant constaté que les formulaires de consentement pour les prêts hypothécaires indiquaient souvent que les dossiers pouvaient être conservés pendant une période précise, et ce, même si le prêt hypothécaire n'avait pas été approuvé par un prêteur. Les formulaires concernant le consentement des clients et la protection de la vie privée de quatre des courtiers vérifiés indiquaient que les agents pouvaient conserver et utiliser les renseignements personnels du demandeur pendant les sept années suivant la présentation de la dernière demande. L'un de ces courtiers avait comme politique de détruire les

demandes de prêt hypothécaire non approuvées dans un délai de six mois, mais une vérification de ses dossiers a montré que cette politique n'avait pas été respectée. Le formulaire du cinquième courtier indiquait que les documents étaient conservés pendant trois ans.

41. Les courtiers en prêts hypothécaires ont été incapables de démontrer pourquoi ils devaient conserver des demandes refusées aussi longtemps. Si les courtiers conservent des renseignements personnels en vue d'une nouvelle utilisation, la LPRPDE les oblige à obtenir de nouveau le consentement du client.

Les pratiques de retrait doivent être renforcées

42. Nous avons également examiné comment les courtiers éliminaient les dossiers qui n'avaient pas abouti à l'obtention d'un prêt hypothécaire. Bien que tous les courtiers possédaient des déchiqueteuses, celles-ci, sauf une exception, coupaient les documents en bandes, ce qui ne détruit pas de manière adéquate les documents contenant des renseignements personnels. Rien ne nous permet de supposer que les déchiqueteuses avaient toujours été utilisées, ni que les courtiers et les agents qui conservaient des dossiers chez eux les détruisaient comme il se doit. Le CPVP a diffusé des directives concernant le vol d'identité dans lesquelles nous recommandons l'utilisation de déchiqueteuses avec coupe en travers pour détruire les documents qui contiennent des renseignements personnels ou financiers.

43. Nous avons vu un cas où un courtier avait réutilisé d'anciennes demandes de prêt hypothécaire qui contenaient les renseignements personnels d'autres clients. Ces anciennes demandes étaient insérées dans les imprimantes et de nouvelles demandes étaient imprimées au verso. Cette façon de faire pourrait entraîner la communication des renseignements personnels d'un client à une autre personne, sans motif valable.

44. RECOMMANDATION

Les courtiers en prêts hypothécaires vérifiés devraient :

- arrêter la collecte routinière et la conservation de renseignements personnels (p. ex. numéros d'assurance sociale), à moins que cela ne soit nécessaire pour réaliser les fins déterminées conformément à la loi;
- être en mesure de démontrer que les clients ont consenti à la collecte de leurs renseignements personnels. En outre, les courtiers devraient informer les clients de la communication et des utilisations potentielles de leurs renseignements et obtenir le consentement explicite pour les utilisations secondaires de ces renseignements;
- élaborer et mettre en œuvre des politiques et des procédures de conservation des renseignements personnels. Celles-ci devraient préciser que les demandes de prêt hypothécaire non approuvées et les autres dossiers contenant des renseignements personnels doivent être détruits de manière sécuritaire dans un délai raisonnable.

RESPONSABILITÉ ET REDDITION DE COMPTES EN MATIÈRE DE PROTECTION DE LA VIE PRIVÉE

45. Les organisations assujetties à la LPRPDE sont responsables des renseignements personnels qu'elles recueillent. La LPRPDE impose aux organisations qui recueillent des renseignements personnels d'établir clairement qui est responsable de la protection de la vie privée. Afin de s'assurer que ces responsabilités sont comprises par les courtiers, les agents et les clients, les courtiers en prêts hypothécaires doivent avoir

défini clairement qui, au sein de leur organisation, est responsable de la protection des renseignements personnels et du respect de la LPRPDE.

46. Pour évaluer la conformité, nous avons examiné les politiques des courtiers relativement à la protection de la vie privée ainsi que les documents portant sur la responsabilité à ce chapitre (lorsqu'ils étaient disponibles). Nous avons aussi examiné les pratiques en matière de signalement des atteintes à la protection des renseignements personnels. Nous nous sommes intéressés aux pratiques entourant l'embauche de nouveaux agents, avons interrogé des agents, consulté le matériel de formation fourni par les sièges sociaux des courtiers et par les fournisseurs de formation des courtiers et des agents.

Les courtiers en prêts hypothécaires connaissaient mal les rôles en matière de protection de la vie privée

47. Nous avons observé que de nombreuses institutions qui traitent des renseignements personnels, notamment les banques, les compagnies d'assurances et les industries fondées sur les services, désignent un responsable de la protection de la vie privée comme personne-ressource pour toutes les questions qui y ont trait. Comme les courtiers en prêts hypothécaires recueillent des renseignements personnels d'ordre financier, ils sont tenus de désigner une personne chargée :

    - de s'assurer qu'eux-mêmes et leurs employés reçoivent une formation adéquate sur leurs obligations en matière de protection de la vie privée;
    - de définir et d'atténuer les risques liés à la protection de la vie privée;
    - de faire un suivi continu de la conformité à la LPRPDE;
    - de veiller à ce que les politiques et les procédures en place soient adéquates et fonctionnent comme prévu.

48. Tous les courtiers examinés avaient un responsable de la protection de la vie privée. Nous avons cependant constaté que les responsabilités associées à ce rôle étaient mal comprises et que les agents ne savaient pas tous le nom du responsable de la protection de la vie privée, ni à qui s'adresser s'ils avaient des questions à ce sujet ou s'ils se rendaient compte d'une atteinte à la protection des renseignements personnels.

49. Par exemple, un des courtiers vérifiés avait un responsable de la protection de la vie privée, mais il se trouvait au siège social de la maison de courtage plutôt qu'au niveau de la franchise. La politique du siège social indique clairement qu'étant donné que les maisons de courtage sont des franchises qui sont détenues et fonctionnent de manière indépendante, l'entreprise décline toute responsabilité pour les pratiques de ses courtiers en matière de protection de la vie privée.

50. Un autre courtier affirme dans sa politique qu'un responsable a été nommé de manière à ce que la franchise s'acquitte de ses responsabilités en matière de protection de la vie privée. Cependant, lorsque nous avons interrogé le franchisé et lui avons demandé qui était ce responsable, on nous a informés qu'il se trouvait au siège social. L'examen de la politique a révélé que le responsable était en fait le courtier-propriétaire lui-même. Nous en avons conclu que les rôles et les responsabilités liés à la protection de la vie privée auraient besoin d'être précisés.

Les courtiers et les agents ne recevaient aucune formation sur leurs responsabilités en matière de protection de la vie privée

51. La LPRPDE stipule que les employés doivent être informés des pratiques et des politiques en matière de protection de la vie privée. Elle stipule également que les employés doivent comprendre leur rôle dans l'application de ces politiques et qu'ils doivent être capables de les expliquer. Aux termes de la *Loi de 2006 sur les maisons de courtage d'hypothèques, les prêteurs*

hypothécaires et les administrateurs d'hypothèques, les courtiers et les agents en prêts hypothécaires doivent suivre une formation concernant l'octroi de prêts hypothécaires. Nous avons constaté que les courtiers et les agents avaient suivi cette formation sur les prêts hypothécaires, mais aucun agent des maisons de courtage en prêts hypothécaires faisant l'objet de la vérification n'avait reçu une formation officielle et continue sur les pratiques en matière de protection de la vie privée propres à l'entreprise, ni sur ses responsabilités en vertu de la LPRPDE.

Les courtiers ont signalé les atteintes à la protection des renseignements personnels de manière proactive

52. Une atteinte à la protection des renseignements personnels se définit comme la perte de renseignements personnels, la consultation ou la communication non autorisées de tels renseignements par suite de la mise en échec des mesures de sécurité d'une organisation dont il est question à l'annexe 1 de la LPRPDE. Des atteintes peuvent se produire lorsque les renseignements personnels au sujet de consommateurs, de patients, de clients ou d'employés sont volés, perdus ou communiqués par erreur (p. ex. lorsqu'un ordinateur contenant des renseignements personnels est volé ou que des renseignements personnels sont envoyés par erreur aux mauvaises personnes). Cependant, une atteinte à la protection des renseignements personnels peut aussi découler de processus administratifs déficients ou de défaillances opérationnelles. Dans le cas présent, les atteintes étaient dues au vol présumé de centaines de rapports de solvabilité.

53. Même si la LPRPDE n'impose pas d'obligations précises aux organisations en ce qui concerne les atteintes à la protection des renseignements personnels, le CPVP a communiqué des directives aux organisations à cet égard. Nous y indiquons que le signalement des atteintes est un signe de bonnes pratiques en matière de protection de la vie privée et qu'il instaure un climat de confiance à l'égard de l'entreprise. Le document d'orientation énumère quatre mesures à prendre en considération quand on réagit à une atteinte ou à une atteinte présumée à la protection des renseignements personnels : 1) limitation de l'atteinte et évaluation préliminaire; 2) évaluation des risques associés à l'atteinte; 3) signalement aux personnes concernées; 4) prévention d'autres atteintes.

54. Aucun des courtiers en prêts hypothécaires vérifiés n'avait en place des politiques officielles de déclaration des atteintes à la protection des renseignements personnels au moment des vols présumés. Toutefois, ils se sont montrés proactifs en communiquant avec le Commissariat afin de déterminer des moyens de restreindre et d'atténuer les atteintes, et en contactant les personnes touchées. En cours de vérification, un des courtiers a élaboré une politique officielle de déclaration des atteintes à la protection des renseignements personnels.

Les processus d'embauche sont maintenant plus rigoureux

55. Nous avons constaté que les courtiers en prêts hypothécaires ont considérablement resserré leurs processus d'embauche après le signalement des atteintes au Commissariat. Depuis le 1er juillet 2008, en vertu de la *Loi de 2006 sur les maisons de courtage d'hypothèques*, *les prêteurs hypothécaires et les administrateurs d'hypothèques*, toute personne physique ou morale qui mène des activités de courtage en prêts hypothécaires en Ontario doit posséder un permis de la Commission des services financiers de l'Ontario (CSFO), l'organisme provincial chargé de surveiller les entreprises de courtage hypothécaire. Pour obtenir ce permis, les courtiers et les agents doivent suivre un cours, réussir un examen, se soumettre à une vérification des antécédents criminels et satisfaire à certaines autres exigences établies par la CSFO.

56. Avant les atteintes à la protection des renseignements personnels, les courtiers se fondaient principalement sur des entrevues, la connaissance du domaine qu'avait le candidat et les références pour embaucher un employé. Ils n'auraient pas nécessairement contacté les prêteurs avec lesquels le candidat faisait affaire. Un des courtiers ne vérifiait pas toujours si le candidat possédait un permis de la CSFO.

57. Depuis les atteintes, un des courtiers a commencé à s'assurer qu'un gestionnaire régional rencontre tous les candidats et qu'un cadre supérieur du siège social approuve tous les nouveaux employés. Ce même courtier exige que tous les agents soient officiellement membres de l'Association canadienne des conseillers hypothécaires accrédités. Un autre courtier nous a informés qu'il n'embauchait désormais que des gens qu'il connaissait personnellement. Deux courtiers ont commencé à vérifier toutes les références.

58. Plusieurs courtiers restreignent également l'accès des nouveaux agents au logiciel de production des rapports de solvabilité. L'un d'eux interdit aux nouveaux agents de se servir de ce logiciel pendant au moins 90 jours. Un autre courtier nous a confirmé que la possibilité pour un agent d'avoir accès aux rapports de solvabilité sera évaluée après que cinq demandes de prêt hypothécaire auront été traitées.

59. RECOMMANDATION

Les courtiers en prêts hypothécaires vérifiés devraient :

- désigner clairement un responsable de la formation en matière de protection de la vie privée et du suivi de la conformité à la LPRPDE;
- élaborer et mettre en œuvre des politiques et des procédures en matière de protection de la vie privée afin d'assurer le respect des principes de la LPRPDE, y compris des renseignements qui expliquent les politiques et procédures de l'organisation en matière de traitement de l'information;
- faire en sorte que leur personnel reçoive une formation sur les politiques et procédures organisationnelles, ainsi que sur leurs responsabilités en vertu de la LPRPDE;
- s'assurer que les courtiers en prêts hypothécaires et les clients savent que ces politiques existent et y ont accès facilement.

Conclusion

60. Les courtiers en prêts hypothécaires utilisent une grande quantité de renseignements personnels pour offrir des produits hypothécaires aux clients. La LPRPDE oblige les courtiers à protéger les renseignements qu'ils recueillent contre la communication non autorisée. Les atteintes à la protection des renseignements personnels en question se sont produites parce que les courtiers en prêts hypothécaires ne s'étaient pas acquittés des obligations imposées par la LPRPDE. Ils n'avaient pas mis en place des mesures de contrôle appropriées pour restreindre l'accès aux rapports de solvabilité, et leurs procédures d'embauche n'étaient pas suffisamment rigoureuses.

61. Depuis que les atteintes ont eu lieu, les courtiers ont considérablement resserré leurs processus d'embauche. Cependant, les courtiers que nous avons vérifiés sont incapables de démontrer que la sécurité physique de leurs locaux ou les mesures de contrôle entourant l'accès aux rapports de solvabilité sont adéquates.

62. Nous avons relevé des lacunes liées à l'outil Web qui permet d'obtenir les rapports de solvabilité. Les atteintes à la protection des renseignements personnels signalées au CPVP se sont produites lorsque des agents en hypothèques ont téléchargé des centaines de rapports de solvabilité qui n'étaient pas nécessaires pour traiter des demandes de prêt hypothécaire. Nous avons mis à l'essai l'outil utilisé pour obtenir les rapports de solvabilité et constaté que, malgré les mesures de contrôle en place pour autoriser l'accès au système d'évaluation du crédit, les courtiers en prêts hypothécaires ne pouvaient pas exercer une surveillance proactive, ni être alertés lorsque des activités suspectes se déroulaient, ni fixer une limite quant au nombre de rapports de solvabilité pouvant être téléchargés. Si ces mesures avaient été en place pour prévenir l'accès non autorisé à l'outil Web, le risque d'accès inapproprié aux rapports de solvabilité aurait été atténué.

63. Au cours de la vérification des courtiers, nous n'avons pas observé d'indications claires et répétées concernant la connaissance des enjeux liés à la protection de la vie privée, ainsi que la formation et la responsabilité dans ce domaine. En raison de l'absence de politiques et procédures détaillées sur la protection de la vie privée, et d'indication claire quant à la responsabilité de leur mise en œuvre, aucun des courtiers soumis à la vérification ne s'acquittait totalement de l'obligation de protéger les renseignements personnels de ses clients et d'autres personnes, en conformité avec la LPRPDE.

Au sujet de la vérification

AUTORITÉ

L'article 18 de la LPRPDE autorise la commissaire à la protection de la vie privée à procéder à la vérification des pratiques de gestion des renseignements personnels d'une organisation si elle a des motifs raisonnables de croire qu'il y a infraction à la *Loi*.

OBJECTIF

L'objectif de la vérification était de déterminer si certains courtiers en prêts hypothécaires de l'Ontario avaient élaboré et mis en œuvre des politiques et des procédures pour protéger les renseignements personnels de leurs clients et d'autres personnes.

CRITÈRES

Nous nous attendions à ce que les courtiers en prêts hypothécaires soumis à la vérification aient mis en œuvre des politiques et des procédures conformes aux exigences des principes sur la collecte, l'utilisation, la conservation et la communication qui sont énoncés à l'annexe 1 de la LPRPDE (la liste complète des principes que nous avons pris en considération dans le cadre de la vérification figure à l'annexe B du présent rapport). Plus précisément, la LPRPDE exige que :

- les fins auxquelles des renseignements personnels sont recueillis soient déterminées avant la collecte ou au moment de celle-ci;
- le consentement de la personne concernée soit obtenu avant la collecte, l'utilisation ou la communication des renseignements personnels;
- le courtier ne recueille que les renseignements personnels nécessaires aux fins déterminées;
- les renseignements personnels ne soient utilisés ou communiqués qu'aux fins pour lesquelles ils ont été recueillis, à moins que la personne concernée n'y consente ou que la loi ne l'exige;
- les renseignements personnels ne soient conservés qu'aussi longtemps que nécessaire.

Conformément au principe sur les mesures de sécurité de la LPRPDE, les courtiers en prêts hypothécaires soumis à la vérification sont tenus d'avoir des mesures appropriées pour protéger les renseignements personnels qu'ils détiennent.

Enfin, conformément au principe sur la responsabilité de la LPRPDE, les courtiers en prêts hypothécaires doivent avoir :

- élaboré et revu régulièrement leurs politiques sur la protection de la vie privée;
- élaboré et mis en œuvre un mécanisme de signalement des atteintes à la protection des renseignements personnels;
- défini les rôles et assigné les responsabilités relativement au respect de la vie privée dans l'ensemble de l'organisation, y compris une formation pertinente;
- établi un moyen pour surveiller leur conformité à la LPRPDE.

PORTÉE ET APPROCHE

La vérification a débuté par un examen des pratiques et des procédures dans le secteur canadien des courtiers en prêts hypothécaires. Cette étape a compris des discussions avec l'Association canadienne des conseillers hypothécaires accrédités et l'Independent Mortgage Brokers Association, et l'examen d'un échantillonnage des dossiers provenant des trois courtiers en prêts hypothécaires qui ont été soumis à une vérification et qui avaient signalé une atteinte à la protection des renseignements personnels au Commissariat.

Sur les 14 courtiers qui avaient signalé au Commissariat une atteinte à la protection des renseignements personnels, nous avons examiné les politiques, systèmes, contrôles administratifs et mesures de sécurité de cinq franchisés situés en Ontario, de même que ceux des sièges sociaux nationaux situés à Toronto et à Vancouver. Ces courtiers ont été choisis en fonction du nombre de personnes touchées, de la nature de l'atteinte et du type de courtage. Nous avons interrogé le personnel et examiné les politiques et les procédures, les ententes, les documents sur le déroulement des processus, les documents sur la conservation des dossiers, le matériel de formation, les systèmes de TI et un échantillon de dossiers de tous les courtiers.

Nous avons rencontré des représentants de la Commission des services financiers de l'Ontario pour avoir une idée plus précise du contexte réglementaire dans lequel les courtiers en prêts hypothécaires exercent leurs activités. Nous avons également rencontré un représentant de la Sous-direction des infractions commerciales de la GRC (Contrefaçon et Fraude d'identité) pour qu'on nous donne un aperçu des circonstances dans lesquelles les atteintes se sont produites. Enfin, nous avons tenu une téléconférence avec l'un des formateurs responsables de la formation des courtiers et des agents en prêts hypothécaires, et nous avons examiné le matériel de cours.

Le travail de vérification était terminé pour l'essentiel le 31 décembre 2009.

NORMES

La vérification a été effectuée en conformité avec les pratiques, les politiques et le mandat législatif du Commissariat à la protection de la vie privée du Canada, et conformément à l'esprit des normes de vérification recommandées par l'Institut canadien des comptables agréés.

ÉQUIPE DE LA VÉRIFICATION

Directeur général : Steven Morgan

Leslie Fournier-Dupelle
Garth Cookshaw
Michael Fagan
Bill Wilson

Annexe A

RECOMMANDATIONS ET RÉPONSES

RECOMMANDATION

Les courtiers en prêts hypothécaires vérifiés devraient protéger les renseignements personnels dont ils sont responsables en mettant en place des mesures de sécurité correspondant à leur degré de sensibilité. Il peut s'agir de s'assurer, sans s'y limiter, que :

- des mesures de sécurité physique adéquates sont en place, comme des alarmes et des classeurs pouvant être verrouillés;
- des mesures supplémentaires sont prises pour protéger les rapports de solvabilité et limiter le nombre de rapports pouvant être téléchargés.

Le Courtier 1 a accepté cette recommandation et s'est engagé à classer tous les dossiers de demande de prêt hypothécaire des clients, que la demande ait été approuvée ou non, dans un classeur en métal fermant à clé. Les agents ont été informés que les dossiers sur lesquels ils travaillaient à la maison devaient être conservés en lieu sûr jusqu'à ce qu'ils soient rapportés au bureau. Par ailleurs, les agents n'ont pas accès aux rapports de solvabilité. Ils doivent plutôt demander au courtier principal d'obtenir le rapport pour eux après avoir fait signer au client un formulaire de consentement. Enfin, le courtier s'est engagé à aviser tous les agents que la consultation d'un rapport de solvabilité crée un nouveau dossier dans leur « fichier Internet temporaire », et que celui-ci doit être effacé après la consultation du rapport.

Le Courtier 2 a accepté cette recommandation, et il s'assurera que tous les dossiers sont conservés sous clé dans un classeur situé dans un bureau particulier à l'intérieur de l'immeuble et que seul le courtier principal y aura accès. De plus, le courtier a centralisé la responsabilité des rapports de solvabilité, de sorte qu'une seule personne a accès à l'outil permettant d'obtenir des rapports de solvabilité.

Le Courtier 3 a accepté cette recommandation et confirmé que toutes les portes de ses locaux actuels sont munies de serrures et que tous les dossiers sont conservés dans un classeur et des tiroirs verrouillés. Le courtier a l'intention de mettre en œuvre une politique en matière de rangement du bureau. En ce qui concerne l'outil d'évaluation du crédit, le courtier a confirmé qu'il surveille l'ensemble des agents en vérifiant au hasard leur historique de recherches auprès des agences d'évaluation du crédit et leur utilisation de l'outil. Les nouveaux agents devront avoir travaillé 90 jours pour l'entreprise et conclu quatre demandes de prêts hypothécaires sous la supervision du courtier principal avant d'être autorisés à télécharger des rapports de solvabilité. Enfin, tous les agents reçoivent un formulaire supplémentaire qu'ils doivent joindre aux contrats du courtier ou de l'agent. Ce formulaire indique qu'ils doivent effacer quotidiennement leurs fichiers temporaires, car ils peuvent contenir des renseignements confidentiels sur les clients. Il devra être signé et être versé au dossier.

Le Courtier 4 a accepté cette recommandation et s'est engagé à ce que tous les dossiers, une fois complétés, soient conservés dans des classeurs verrouillés. De plus, le courtier a confirmé que tous les ordinateurs sont protégés par un mot de passe et sont configurés de manière à supprimer automatiquement les fichiers

temporaires. Le courtier a affirmé que l'édifice est surveillé 24 heures par jour, sept jours par semaine par plus de 30 caméras. En dehors des heures de travail, des gardiens de sécurité sont en poste, et il faut un laissez-passer pour entrer dans l'édifice et accéder à chacun des étages. Le courtier s'est aussi engagé à installer, au cours des six prochains mois, des caméras et un système d'alarme qui pourront être surveillés à l'extérieur de l'édifice en tout temps. Bien que les agents puissent télécharger des rapports de solvabilité au moyen de l'outil Web, le courtier a instauré une politique interdisant aux nouveaux agents de télécharger ces rapports pendant les 90 premiers jours de leur emploi. Enfin, le courtier évalue actuellement la possibilité de confier à une seule personne la vérification de la solvabilité.

RECOMMANDATION

Les courtiers en prêts hypothécaires vérifiés devraient :

- arrêter la collecte routinière et la conservation de renseignements personnels (p. ex. numéros d'assurance sociale), à moins que cela ne soit nécessaire pour réaliser les fins déterminées conformément à la loi;
- être en mesure de démontrer que les clients ont consenti à la collecte de leurs renseignements personnels. En outre, les courtiers devraient informer les clients de la communication et des utilisations potentielles de leurs renseignements et obtenir le consentement explicite pour les utilisations secondaires de ces renseignements;
- élaborer et mettre en œuvre des politiques et des procédures de conservation des renseignements personnels. Celles-ci devraient préciser que les demandes de prêt hypothécaire non approuvées et les autres dossiers contenant des renseignements personnels doivent être détruits de manière sécuritaire dans un délai raisonnable.

Le Courtier 1 a accepté cette recommandation, et il reconnaît qu'il recueille régulièrement des renseignements personnels sur les demandeurs afin de traiter leurs demandes de prêt. Ces renseignements peuvent comprendre le numéro d'assurance sociale. Le courtier a expliqué que les prêteurs demandent fréquemment le NAS pour s'assurer que le rapport de solvabilité obtenu concerne la bonne personne. De plus, le courtier a confirmé que certains prêteurs exigent le NAS dans le cadre du processus d'approbation pour déterminer si le demandeur est un résident non permanent. En ce qui concerne la question du consentement, le courtier confirme que tous les demandeurs signent une demande de prêt hypothécaire, dans laquelle il est indiqué qu'ils consentent à ce que des renseignements personnels soient recueillis aux fins du traitement de la demande. Le courtier s'assure que les clients acceptent également de recevoir à l'occasion du matériel de marketing direct lié au crédit hypothécaire et aux affaires immobilières. Enfin, le courtier s'est engagé à clarifier ses lignes directrices en matière de protection de la vie privée pour faire en sorte que les demandes de prêts hypothécaires non approuvées soient détruites de manière sécuritaire dans un délai de six mois.

Le Courtier 2 a accepté cette recommandation, et il a déclaré que ces mesures avaient été mises en place depuis la vérification. Il a affirmé que, bien qu'il utilise les formulaires de consentement types fournis par l'outil sur l'évaluation du crédit, il évaluera la possibilité d'offrir l'option de ne pas consentir aux usages secondaires des renseignements personnels. Une fois que ces pratiques auront été instaurées, le courtier s'est engagé à ce qu'il y ait une formation suivie et à ce que les dossiers soient examinés chaque semaine pour s'assurer que les renseignements sont exacts et que l'on se conforme aux politiques.

Le Courtier 3 a accepté cette recommandation, et il veillera à ce que le formulaire de demande de prêt hypothécaire soit modifié pour indiquer qu'il n'est pas obligatoire de fournir son NAS. En ce qui concerne les demandes faites par téléphone, le courtier s'est engagé à informer les clients de vive voix qu'il n'est pas essentiel de fournir leur NAS. Il s'est aussi engagé

à ce que cette politique soit incluse dans les formulaires de formation remis aux agents. Le courtier a mis en œuvre une politique exigeant que les demandes de prêts hypothécaires non approuvées soient déchiquetées dans un délai d'une semaine et que les autres dossiers soient conservés dans un classeur en métal verrouillé. En ce qui a trait au consentement, le courtier a déclaré que le logiciel qu'il utilise lui permet de connaître la date, l'heure et la forme (p. ex. verbale) du consentement donné par le client. Lorsque le consentement aura été donné de vive voix pour l'obtention du rapport de solvabilité, le courtier veillera à ce que le client signe après coup un formulaire de consentement confirmant qu'il a consenti à ce que l'on consulte son rapport de solvabilité.

Le Courtier 4 a accepté cette recommandation tout en affirmant que le NAS est le meilleur moyen de s'assurer d'obtenir le bon rapport de solvabilité. Le courtier s'engage à faire signer aux clients un formulaire de consentement avant d'obtenir leur rapport de solvabilité; ce formulaire indiquera clairement quels renseignements personnels seront utilisés et à qui ils seront communiqués. Le formulaire sera modifié pour inclure une option de consentement donnant aux clients davantage de contrôle sur les usages secondaires. Le courtier confirme que les demandes sur support papier non approuvées ou annulées sont déchiquetées dans un délai de 30 jours et que les dossiers papier datant de plus de trois ans sont détruits de manière sécuritaire. Enfin, le courtier affirme qu'il ne réutilise plus les demandes de prêt hypothécaire comme papier brouillon.

RECOMMANDATION

Les courtiers en prêts hypothécaires vérifiés devraient :

- désigner clairement un responsable de la formation en matière de protection de la vie privée et du suivi de la conformité à la LPRPDE;
- élaborer et mettre en œuvre des politiques et des procédures en matière de protection de la vie privée afin d'assurer le respect des principes de la LPRPDE, y compris des renseignements qui expliquent les politiques et procédures de l'organisation en matière de traitement de l'information;
- faire en sorte que leur personnel reçoive une formation sur les politiques et procédures organisationnelles, ainsi que sur leurs responsabilités en vertu de la LPRPDE;
- s'assurer que les courtiers en prêts hypothécaires et les clients savent que ces politiques existent et y ont accès facilement.

Le Courtier 1 a accepté cette recommandation et il confirme qu'il est responsable des politiques, de la formation et de la conformité de l'entreprise en ce qui a trait à la protection des renseignements personnels. Le courtier a indiqué que le manuel des politiques et des procédures, dont chaque agent reçoit un exemplaire que l'on passe en revue avec lui, contient des

directives sur la protection des renseignements personnels des clients. Le courtier a confirmé que ces directives ont été examinées en détail avec chacun des agents et que l'on insiste régulièrement sur l'importance de la conformité dans le cours des activités de l'entreprise. Le courtier s'est engagé à revoir et à mettre à jour ces directives dans les 30 prochains jours pour tenir compte des recommandations formulées dans le présent rapport. Plus précisément, le courtier s'est engagé à élargir la formation des agents afin d'apporter des éclaircissements sur leurs responsabilités personnelles en matière de protection de la vie privée. Pour ce faire, le courtier a dit qu'il utilisera les ressources du site Web du Commissariat à la protection de la vie privée, et il exigera que chaque agent reconnaisse être informé au sujet des directives de l'entreprise relativement à la protection de la vie privée et de ses responsabilités personnelles.

Le Courtier 2 a accepté cette recommandation, et il a récemment engagé un agent de formation et de la conformité pour donner de la formation aux employés sur leurs responsabilités en matière de protection de la vie privée. Le courtier s'est engagé à agir avec diligence pour s'assurer que les procédures appropriées sont suivies en tout temps.

Le Courtier 3 a accepté cette recommandation, et il se chargera de la formation sur la protection de la vie privée et de la surveillance de la conformité à la LPRPDE. Le courtier s'est engagé à répondre aux questions ou aux préoccupations des agents et des clients relativement à la protection de la vie privée, et à élaborer un manuel des politiques et des procédures pour garantir la conformité à la LPRPDE. Ce manuel sera mis à la disposition de tous les agents, qui devront accepter de suivre les procédures qui y sont indiquées. De plus, le manuel des procédures et la politique sur la protection de la vie privée seront affichés sur le site Web du courtier, et une version imprimée sera disponible pour les clients.

Le Courtier 4 a accepté cette recommandation, et il s'est engagé à veiller à ce que tous les agents reçoivent une formation sur la conformité aux principes de respect de la vie privée et qu'il y ait un suivi continu. Le courtier est en voie d'élaborer un manuel destiné aux agents, dans lequel sont décrites leurs responsabilités en vertu de la LPRPDE. La politique du courtier en matière de protection de la vie privée est affichée sur son site Web. Enfin, le courtier a affirmé qu'il mettait à jour ses politiques et procédures pour tenir compte des recommandations énoncées dans le présent rapport, et que ce travail sera terminé d'ici six mois.

Annexe B

PRINCIPES DE L'ANNEXE 1 DE LA LPRPDE PRIS EN CONSIDÉRATION PENDANT LA VÉRIFICATION

4.1 PREMIER PRINCIPE — RESPONSABILITÉ

Une organisation est responsable des renseignements personnels dont elle a la gestion et doit désigner une ou des personnes qui devront s'assurer du respect des principes énoncés ci-dessous.

4.1.1

Il incombe à la ou aux personnes désignées de s'assurer que l'organisation respecte les principes même si d'autres membres de l'organisation peuvent être chargés de la collecte et du traitement quotidiens des renseignements personnels. D'autres membres de l'organisation peuvent aussi être délégués pour agir au nom de la ou des personnes désignées.

4.1.2

Il doit être possible de connaître sur demande l'identité des personnes que l'organisation a désignées pour s'assurer que les principes sont respectés.

4.1.3

Une organisation est responsable des renseignements personnels qu'elle a en sa possession ou sous sa garde, y compris les renseignements confiés à une tierce partie aux fins de traitement. L'organisation doit, par voie contractuelle ou autre, fournir un degré comparable de protection aux renseignements qui sont en cours de traitement par une tierce partie.

4.1.4

Les organisations doivent assurer la mise en œuvre des politiques et des pratiques destinées à donner suite aux principes, y compris :

a) la mise en œuvre des procédures pour protéger les renseignements personnels;

b) la mise en place des procédures pour recevoir les plaintes et les demandes de renseignements et y donner suite;

c) la formation du personnel et la transmission au personnel de l'information relative aux politiques et pratiques de l'organisation; et

d) la rédaction des documents explicatifs concernant leurs politiques et procédures.

4.2 DEUXIÈME PRINCIPE — DÉTERMINATION DES FINS DE LA COLLECTE DES RENSEIGNEMENTS

Les fins auxquelles des renseignements personnels sont recueillis doivent être déterminées par l'organisation avant la collecte ou au moment de celle-ci.

4.2.1

L'organisation doit documenter les fins auxquelles les renseignements personnels sont recueillis afin de se conformer au principe de la transparence (article 4.8) et au principe de l'accès aux renseignements personnels (article 4.9).

4.2.2

Le fait de préciser les fins de la collecte de renseignements personnels avant celle-ci ou au moment de celle-ci permet à l'organisation de déterminer les renseignements dont elle a besoin pour réaliser les fins mentionnées. Suivant le principe de la limitation en matière de collecte (article 4.4), l'organisation ne doit recueillir que les renseignements nécessaires aux fins mentionnées.

4.2.3

Il faudrait préciser à la personne auprès de laquelle on recueille des renseignements, avant la collecte ou au moment de celle-ci, les fins auxquelles ils sont destinés. Selon la façon dont se fait la collecte, cette précision peut être communiquée de vive voix ou par écrit. Par exemple, on peut indiquer ces fins sur un formulaire de demande de renseignements.

4.2.4

Avant de se servir de renseignements personnels à des fins non précisées antérieurement, les nouvelles fins doivent être précisées avant l'utilisation. À moins que les nouvelles fins auxquelles les renseignements sont destinés ne soient prévues par une loi, il faut obtenir le consentement de la personne concernée avant d'utiliser les renseignements à cette nouvelle fin. Pour obtenir plus de précisions sur le consentement, se reporter au principe du consentement (article 4.3).

4.2.5

Les personnes qui recueillent des renseignements personnels devraient être en mesure d'expliquer à la personne concernée à quelles fins sont destinés ces renseignements.

4.2.6

Ce principe est étroitement lié au principe de la limitation de la collecte (article 4.4) et à celui de la limitation de l'utilisation, de la communication et de la conservation (article 4.5).

4.3 TROISIÈME PRINCIPE — CONSENTEMENT

Toute personne doit être informée de toute collecte, utilisation ou communication de renseignements personnels qui la concernent et y consentir, à moins qu'il ne soit pas approprié de le faire. Note : Dans certaines circonstances, il est possible de recueillir, d'utiliser et de communiquer des renseignements à l'insu de la personne concernée et sans son consentement. Par exemple, pour des raisons d'ordre juridique ou médical ou pour des raisons de sécurité, il peut être impossible ou peu réaliste d'obtenir le consentement de la personne concernée. Lorsqu'on recueille des renseignements aux fins du contrôle d'application de la loi, de la détection d'une fraude ou de sa prévention, on peut aller à l'encontre du but visé si l'on cherche à obtenir le consentement de la personne concernée. Il peut être impossible ou inopportun de chercher à obtenir le consentement d'un mineur, d'une personne gravement malade ou souffrant d'incapacité mentale. De plus, les organisations qui ne sont pas en relation directe avec la personne concernée ne sont pas toujours en mesure d'obtenir le consentement prévu. Par exemple, il peut être peu réaliste pour une œuvre de bienfaisance ou une entreprise de marketing direct souhaitant acquérir une liste d'envoi d'une autre organisation de chercher à obtenir le consentement des personnes concernées. On s'attendrait, dans de tels cas, à ce que l'organisation qui fournit la liste obtienne le consentement des personnes concernées avant de communiquer des renseignements personnels.

4.3.1

Il faut obtenir le consentement de la personne concernée avant de recueillir des renseignements personnels à son sujet et d'utiliser ou de communiquer les renseignements recueillis. Généralement, une organisation obtient le consentement des personnes concernées relativement à l'utilisation et à la communication des renseignements personnels au moment de la collecte. Dans certains cas, une organisation peut obtenir le consentement concernant l'utilisation ou la communication des renseignements après avoir recueilli ces renseignements, mais avant de s'en servir, par exemple, quand elle veut les utiliser à des fins non précisées antérieurement.

4.3.2

Suivant ce principe, il faut informer la personne au sujet de laquelle on recueille des renseignements et obtenir son consentement. Les organisations doivent faire un effort raisonnable pour s'assurer que la personne est informée des fins auxquelles les renseignements seront utilisés. Pour que le consentement soit valable, les fins doivent être énoncées de façon que la personne puisse raisonnablement comprendre de quelle manière les renseignements seront utilisés ou communiqués.

4.3.3

Une organisation ne peut pas, pour le motif qu'elle fournit un bien ou un service, exiger d'une personne qu'elle consente à la collecte, à l'utilisation ou à la communication de renseignements autres que ceux qui sont nécessaires pour réaliser les fins légitimes et explicitement indiquées.

4.3.4

La forme du consentement que l'organisation cherche à obtenir peut varier selon les circonstances et la nature des renseignements. Pour déterminer la forme que prendra le consentement, les organisations doivent tenir compte de la sensibilité des renseignements. Si certains renseignements sont presque toujours considérés comme sensibles, par exemple les dossiers médicaux et le revenu, tous les renseignements peuvent devenir sensibles suivant le contexte. Par exemple, les nom et adresse des abonnés d'une revue d'information ne seront généralement pas considérés comme des renseignements sensibles. Toutefois, les nom et adresse des abonnés de certains périodiques spécialisés pourront l'être.

4.3.5

Dans l'obtention du consentement, les attentes raisonnables de la personne sont aussi pertinentes. Par exemple, une personne qui s'abonne à un périodique devrait raisonnablement s'attendre à ce que l'entreprise, en plus de se servir de son nom et de son adresse à des fins de postage et de facturation, communique avec elle pour lui demander si elle désire que son abonnement soit renouvelé. Dans ce cas, l'organisation peut présumer que la demande de la personne constitue un consentement à ces fins précises. D'un autre côté, il n'est pas raisonnable qu'une personne s'attende à ce que les renseignements personnels qu'elle fournit à un professionnel de la santé soient donnés sans son consentement à une entreprise qui vend des produits de soins de santé. Le consentement ne doit pas être obtenu par un subterfuge.

4.3.6

La façon dont une organisation obtient le consentement peut varier selon les circonstances et la nature des renseignements recueillis. En général, l'organisation devrait chercher à obtenir un consentement explicite si les renseignements sont susceptibles d'être considérés comme sensibles. Lorsque les renseignements sont moins sensibles, un consentement implicite serait normalement jugé suffisant. Le consentement peut également être donné par un représentant autorisé (détenteur d'une procuration, tuteur).

4.3.7

Le consentement peut revêtir différentes formes, par exemple :

a) on peut se servir d'un formulaire de demande de renseignements pour obtenir le consentement, recueillir des renseignements et informer la personne de l'utilisation qui sera faite des renseignements. En remplissant le formulaire et en le signant, la personne donne son consentement à la collecte de renseignements et aux usages précisés;

b) on peut prévoir une case où la personne pourra indiquer en cochant qu'elle refuse que ses nom et adresse soient communiqués à d'autres organisations. Si la personne ne coche pas la case, il sera présumé qu'elle consent à ce que les renseignements soient communiqués à des tiers;

c) le consentement peut être donné de vive voix lorsque les renseignements sont recueillis par téléphone; ou

d) le consentement peut être donné au moment où le produit ou le service est utilisé.

4.3.8

Une personne peut retirer son consentement en tout temps, sous réserve de restrictions prévues par une loi ou un contrat et d'un préavis raisonnable. L'organisation doit informer la personne des conséquences d'un tel retrait.

4.4 QUATRIÈME PRINCIPE — LIMITATION DE LA COLLECTE

L'organisation ne peut recueillir que les renseignements personnels nécessaires aux fins déterminées et doit procéder de façon honnête et licite.

4.4.1

Les organisations ne doivent pas recueillir des renseignements de façon arbitraire. On doit restreindre tant la quantité que la nature des renseignements recueillis à ce qui est nécessaire pour réaliser les fins déterminées. Conformément au principe de la transparence (article 4.8), les organisations doivent préciser la nature des renseignements recueillis comme partie intégrante de leurs politiques et pratiques concernant le traitement des renseignements.

4.4.2

L'exigence selon laquelle les organisations sont tenues de recueillir des renseignements personnels de façon honnête et licite a pour objet de les empêcher de tromper les gens et de les induire en erreur quant aux fins auxquelles les renseignements sont recueillis. Cette obligation suppose que le consentement à la collecte de renseignements ne doit pas être obtenu par un subterfuge.

4.4.3

Ce principe est étroitement lié au principe de détermination des fins auxquelles la collecte est destinée (article 4.2) et à celui du consentement (article 4.3).

4.5 CINQUIÈME PRINCIPE— LIMITATION DE L'UTILISATION, DE LA COMMUNICATION ET DE LA CONSERVATION

Les renseignements personnels ne doivent pas être utilisés ou communiqués à des fins autres que celles auxquelles ils ont été recueillis à moins que la personne concernée n'y consente ou que la loi ne l'exige. On ne doit conserver les renseignements personnels qu'aussi longtemps que nécessaire pour la réalisation des fins déterminées.

4.5.1

Les organisations qui se servent de renseignements personnels à des fins nouvelles doivent documenter ces fins (voir article 4.2.1).

4.5.2

Les organisations devraient élaborer des lignes directrices et appliquer des procédures pour la conservation des renseignements personnels. Ces lignes directrices devraient préciser les durées minimales et maximales de conservation. On doit conserver les renseignements personnels servant à prendre une décision au sujet d'une personne suffisamment longtemps pour permettre à la personne concernée d'exercer son droit d'accès à l'information après que la décision a été prise. Une organisation peut être assujettie à des exigences prévues par la loi en ce qui concerne les périodes de conservation.

4.5.3

On devrait détruire, effacer ou dépersonnaliser les renseignements personnels dont on n'a plus besoin aux fins précisées. Les organisations doivent élaborer des lignes directrices et appliquer des procédures régissant la destruction des renseignements personnels.

4.5.4

Ce principe est étroitement lié au principe du consentement (article 4.3), à celui de la détermination des fins auxquelles la collecte est destinée (article 4.2), ainsi qu'à celui de l'accès individuel (article 4.9).

4.7 SEPTIÈME PRINCIPE — MESURES DE SÉCURITÉ

Les renseignements personnels doivent être protégés au moyen de mesures de sécurité correspondant à leur degré de sensibilité.

4.7.1

Les mesures de sécurité doivent protéger les renseignements personnels contre la perte ou le vol ainsi que contre la consultation, la communication, la copie, l'utilisation ou la modification non autorisées. Les organisations doivent protéger les renseignements personnels quelle que soit la forme sous laquelle ils sont conservés.

4.7.2

La nature des mesures de sécurité variera en fonction du degré de sensibilité des renseignements personnels recueillis, de la quantité, de la répartition et du format des renseignements personnels ainsi que des méthodes de conservation. Les renseignements plus sensibles devraient être mieux protégés. La notion de sensibilité est présentée à l'article 4.3.4.

4.7.3

Les méthodes de protection devraient comprendre :

a) des moyens matériels, par exemple le verrouillage des classeurs et la restriction de l'accès aux bureaux; et

c) des mesures techniques, par exemple l'usage de mots de passe et du chiffrement.

4.7.4

Les organisations doivent sensibiliser leur personnel à l'importance de protéger le caractère confidentiel des renseignements personnels.

4.7.5

Au moment du retrait ou de la destruction des renseignements personnels, on doit veiller à empêcher les personnes non autorisées d'y avoir accès (article 4.5.3).