

# VOL D'IDENTITÉ

PROTÉGEZ  
VOTRE  
ENTREPRISE

PROTÉGEZ  
VOS  
CLIENTS

Canada

 Ontario  Québec

 NOVA SCOTIA  New Brunswick

 BRITISH COLUMBIA  Manitoba

 Prince Edward Island  Government of Saskatchewan

 Alberta  GOVERNMENT OF NEWFOUNDLAND AND LABRADOR

 Yukon  Northwest Territories  Nunavut

# Trousse d'information sur le vol d'identité des entreprises

## VOL D'IDENTITÉ :

Identifiez-le.

Signalez-le.

Enrayez-le.

Pour obtenir d'autres conseils et outils au sujet du  
vol d'identité, consultez [cmcweb.ca/volidentite](http://cmcweb.ca/volidentite)



Le centre d'appel antifraude du Canada

Produit par le Comité des mesures en matière  
de consommation fédéral, provincial et territorial

N° de catalogue lu23-7/2005F-PDF  
ISBN 0-662-79031-6  
54238X

*La présente trousse est fournie à titre informatif uniquement, et vise à insister sur la nécessité de mettre en œuvre des politiques et des pratiques efficaces en matière de renseignements personnels. Aucun renseignement contenu dans cette trousse ne doit être interprété comme un conseil juridiques. Pour connaître vos droits et vos obligations juridiques, vous devriez consulter la législation et la réglementation pertinentes, ainsi que votre avocat.*

<b>1) VOL D'IDENTITÉ : UN ENJEU POUR LES ENTREPRISES ET LEURS CLIENTS</b> .....	1
Qu'entend-on par renseignements personnels? .....	2
Pourquoi les entreprises doivent-elles les protéger? .....	2
Risques accrus .....	2
Confiance et fidélité des clients .....	3
<b>2) CONSEILS POUR RÉDUIRE LES RISQUES</b> .....	4
Étudiez les pratiques au sein de votre entreprise .....	4
Collecte des renseignements personnels .....	5
Utilisation .....	7
Divulgence .....	8
Sécurité et stockage des données .....	9
Élimination .....	11
Le personnel et la sécurité des données .....	12
Modifiez vos pratiques .....	13
<b>3) QUE FAIRE EN CAS D'INTRUSION</b> .....	14
Mesures à prendre lorsque les renseignements sont compromis .....	14
Enquêter sur l'incident .....	14
Informez les clients et les organisations externes .....	14
Communiquer avec les médias .....	16
<b>4) OUTILS : COMMENT INFORMER LES CLIENTS DU VOL DE RENSEIGNEMENTS PERSONNELS</b> .....	17
Modèle de lettre de notification .....	17
Que dire et comment réagir en cas d'intrusion :	
Questions et réponses types .....	19



# 1. VOL D'IDENTITÉ: UNE PRIORITÉ POUR LES ENTREPRISES ET LEURS CLIENTS

Selon les organismes chargés de l'application de la loi, parmi les crimes auxquels les consommateurs, les entreprises et les gouvernements ont à faire face, le vol d'identité est celui qui connaît la croissance la plus rapide. Le nombre de vols perpétrés à l'interne augmentent : de plus en plus souvent, ce sont des criminels au sein des organisations qui volent les renseignements personnels des clients. Les entreprises peuvent préserver leur réputation et éviter des pertes financières en planifiant et en mettant en œuvre des politiques qui permettent de protéger les renseignements personnels de leurs clients.

La plupart des entreprises recueillent et conservent des renseignements personnels, mais combien ont mis en place un plan pour les collecter et les conserver en toute sécurité? Votre entreprise a-t-elle un tel plan? Considérez ce qui suit :

- un seul ordinateur peut renfermer des dossiers sur des milliers de clients;
- un classeur non verrouillé peut renfermer des codes d'accès et des numéros de comptes ou de permis qu'une société partage avec ses partenaires, ses fournisseurs ou ses vendeurs;
- les entrepreneurs externes retenus pour bâtir et gérer des bases de données peuvent voir et copier des renseignements sur les clients d'une entreprise, notamment les numéros de cartes de crédit et même, parfois, les numéros de permis de conduire.

La législation relative à la protection de la vie privée exige que toutes les entreprises mettent en place des systèmes pour s'assurer que les renseignements sur les clients sont conservés en toute sécurité, sont exacts, sont recueillis avec le consentement des clients et ne sont pas utilisés à d'autres fins que celles déclarées. La *Loi sur la protection des renseignements personnels et les documents électroniques* (LPRPDE) du gouvernement fédéral s'applique aux entreprises qui exercent une activité dans les provinces et les territoires qui ne disposent pas de lois similaires. Le Québec, la Colombie-Britannique, et l'Alberta ont des lois similaires. Ce guide vous aidera à élaborer un plan qui vous permettra d'éviter le vol de renseignements, et vous fournit des conseils sur ce que vous devez faire dans le cas où vos renseignements ont été volés.

---

***Vol d'identité :  
Identifiez-le.  
Signalez-le.  
Enrayez-le.***

## Qu'entend-on par renseignements personnels?

Tous les renseignements factuels ou subjectifs, enregistrés ou non, sur une personne identifiable constituent des renseignements personnels. Il peut s'agir de divers renseignements, par exemple : le nom, l'adresse, l'âge, le sexe, des numéros d'identification ou de cartes de crédit, les revenus, l'emploi, les biens, les dettes, les dossiers de paiement, les références personnelles et les dossiers médicaux. Habituellement, les renseignements personnels *ne comprennent pas* les coordonnées d'un employé à son lieu de travail, mais peuvent inclure l'adresse de courrier électronique de l'employé. En règle générale, les renseignements recueillis sur les clients et sur les employés ne doivent être utilisés qu'aux fins pour lesquelles ils ont été obtenus ou à d'autres fins auxquelles les personnes concernées ont consenti.

## Qu'est-ce que le vol d'identité (fraude)?

Le vol d'identité survient lorsque quelqu'un obtient et utilise les renseignements personnels d'une autre personne à son insu ou sans son consentement pour commettre une fraude qui rapportera un gain financier ou pour tout autre acte criminel.

Un voleur n'a pas besoin de beaucoup de renseignements pour voler l'identité d'une victime et perturber gravement sa vie : comme point de départ, il suffit souvent du nom, de l'adresse et de la date de naissance.

## Pourquoi les entreprises doivent-elles protéger les renseignements personnels?

**Risques accrus.** Le vol d'identité connaît une croissance rapide. Chaque année, les renseignements personnels de milliers de victimes sont utilisés par des criminels pour commettre des fraudes financières, notamment pour ouvrir de faux comptes sous un

autre nom. Le nombre de crimes de ce type augmente parce qu'on recueille et conserve aujourd'hui plus de renseignements qu'auparavant, et les risques de vol se multiplient chaque fois que des renseignements sont transmis, conservés ou éliminés de manière non sécuritaire. Un nombre inquiétant de vols d'identité sont perpétrés à l'interne, par des personnes qui ont accès aux données confidentielles détenues par l'entreprise.

#### **Confiance et fidélité des clients.**

Les consommateurs commencent à s'inquiéter d'avoir à donner des renseignements, et en apprennent davantage chaque jour sur leurs droits en matière de protection de la vie privée. Ils tiennent de plus en plus les organisations responsables de la protection de leurs renseignements personnels – non seulement sur le plan juridique, mais également sur le marché. Si les entreprises perdent la confiance des consommateurs et subissent une baisse de l'achalandage, leurs résultats financiers en subiront les conséquences.

### Gérer de façon à empêcher la criminalité interne \*

Des centaines de clients sans méfiance d'une station-service de l'île de Vancouver qui utilisaient leur carte de débit pour payer l'essence achetée ont été choqués d'apprendre que leurs numéros d'identification personnel (NIP) et le numéro de leurs cartes étaient enregistrés deux fois : une fois pour la transaction, une fois au bénéfice d'un voleur.

Lorsque que les policiers ont fini par arrêter un ancien employé, 178 accusations d'utilisation frauduleuse de données ont été portées contre lui. Le montant de la fraude dépassait 200 000 \$. Il avait copié les données des cartes de débit au moment où il les glissait dans le lecteur.

Conformément au *Code de pratique canadien de services de carte de débit*, les victimes ont été remboursées par leurs institutions financières. On a averti la station-service que son accès aux services de paiement en ligne serait annulé si elle ne prenait pas des mesures de sécurité adéquates.

Pour prévenir d'autres vols, le propriétaire a mis en place de nouvelles procédures. Il a resserré le processus de sélection et de vérification des antécédents lors de l'embauche d'employés, il a aussi commencé à vérifier ses appareils pour s'assurer que personne ne les avait altérés.

\* Toutes les anecdotes relatées dans les encadrés marginaux sont vraies. Seuls les noms, les lieux et d'autres détails mentionnés ont été changés.

---

## 2. CONSEILS POUR RÉDUIRE LES RISQUES

### Étudiez les pratiques au sein de votre entreprise

Toutes les organisations doivent gérer le « cycle de vie » des renseignements personnels qu'elles recueillent. Le vol peut être perpétré par des personnes de l'extérieur qui réussissent à avoir accès aux renseignements; il peut aussi être l'œuvre de quelqu'un à l'interne. Une bonne stratégie de sécurité doit prévoir des mesures contre les deux possibilités.

**Consacrez du temps à la protection des renseignements personnels.** Désignez quelqu'un qui sera chargé de superviser la gestion et la sécurité des renseignements, ou assumez vous-même cette responsabilité.

La personne responsable de la protection des renseignements personnels et de la sécurité doit évaluer :

- les processus en place pour recueillir, traiter, stocker et éliminer les données électroniques et sur papier;
- la protection des systèmes informatiques, comme les pare-feu et les pistes de vérification;
- le rôle et le niveau de sécurité des personnes qui ont accès aux renseignements sur le personnel et sur les clients;
- comment faire connaître vos politiques aux clients et au public et quoi leur dire en cas de vol de renseignements.

Pour une entreprise, la collecte et l'utilisation de renseignements personnels comportent habituellement cinq aspects principaux : **la collecte, l'utilisation, la divulgation, la sécurité et le stockage des données**, ainsi que **l'élimination**.

## Collecte

**Sachez ce que vous recueillez et dans quel but.** Passez en revue tous les renseignements personnels recueillis par votre organisation dans le cadre de transactions ainsi qu'à d'autres moments. Recueillez-vous des données sur vos clients? Déterminez les fins pour lesquelles les renseignements sont recueillis, informez les clients en ce sens, et obtenez leur consentement. Assurez-vous que vos employés peuvent expliquer les fins pour lesquelles ils recueillent les renseignements.

**Si vous n'en avez pas besoin, ne les recueillez pas.** Beaucoup d'entreprises recueillent plus d'informations que ce dont elles ont besoin, particulièrement lorsqu'elles demandent à leurs clients de remplir des formulaires. Envisagez de ne pas demander l'adresse, l'adresse électronique et le numéro de téléphone si vous n'avez besoin que du nom. Le numéro d'assurance sociale (NAS) est un numéro confidentiel que le client n'est tenu de déclarer que lorsqu'il reçoit des revenus (par un emploi ou des investissements), aux fins de déclaration d'impôts. Autrement, il ne devrait pas être demandé.

### Recueillez seulement les\* données dont vous avez besoin

Chaque fois que les employés du club de location de vidéos local situé au centre-ville de Winnipeg ouvraient un compte client, ils demandaient le numéro d'une carte de crédit et celui du permis de conduire du client, son adresse et son numéro de téléphone. Les propriétaires n'ont jamais vraiment réfléchi à l'importance de ces données. Ils n'ont donc jamais pensé que le fait de les conserver aurait comme conséquence que 26 clients perdraient chacun des milliers de dollars ... ce qui est arrivé!

Les données conservées dans leur système informatique n'étaient ni protégées par un mot de passe ni cryptées. Un jour, un voleur est entré par effraction et s'est emparé de la base de données. Il a alors entrepris un magasinage effréné. Heureusement, il a été appréhendé par les policiers et les clients n'ont pas eu à payer les frais frauduleux.

Aujourd'hui, au club vidéo, on évite de recueillir les numéros de permis de conduire. Par ailleurs, l'accès à leurs systèmes est protégé par un mot de passe et des pare-feu empêchent l'accès à leur base de données. On remet aussi aux clients un court document d'une page décrivant leur politique de confidentialité et leurs pratiques en matière de sécurité des renseignements.

*\* Toutes les anecdotes relatées dans les encadrés marginaux sont vraies. Seuls les noms, les lieux et d'autres détails mentionnés ont été changés.*

**Les renseignements personnels ne doivent pas être à la vue de tous.** Les personnes qui font la queue à votre bureau ou à votre magasin peuvent-elles entendre les clients qui donnent leur numéro de téléphone ou leur mot de passe à vos employés? Donnez instruction aux employés qui doivent obtenir des renseignements personnels de parler de façon discrète. Placez les écrans des ordinateurs de façon à ce qu'ils ne puissent être vus que par l'utilisateur.

**Protégez les cartes des clients.** Quand les clients font des achats, assurez-vous qu'ils peuvent entrer leur numéro d'identification personnel (NIP) sans qu'il soit possible de les observer. Installez des plaquettes de protection sur les terminaux et faites des vérifications régulières pour vous assurer que l'équipement n'a pas été altéré. Placez les caméras vidéo de surveillance de façon à ce qu'il soit impossible d'enregistrer les clients qui entrent leur NIP.

**Vérifiez les cartes.** Le personnel devrait s'assurer que les clients sont bien qui ils prétendent être en comparant la signature à celle qui se trouve au verso de la carte et, au besoin, en demandant une pièce d'identité avec photo. Envisagez d'utiliser des appareils qui tronquent les numéros des cartes de débit et de crédit à l'impression des reçus (c.-à-d. qui n'impriment qu'une partie du numéro de carte, afin d'améliorer la protection offerte aux consommateurs. Ne prenez pas en note des numéros de cartes dont vous n'avez pas besoin.

**Surveillez le crédit.** Si vous accordez du crédit à certains clients, surveillez les écarts ou les changements récents d'adresse du demandeur. Prenez des mesures supplémentaires pour vérifier l'identité de la personne : par exemple, n'hésitez pas à demander d'autres pièces d'identité. S'il y a une alerte de fraude dans le dossier de crédit du client, les agences de renseignements de crédit vous donneront le numéro de téléphone confirmé du client pour vous permettre de vérifier la validité de la demande.

**Sécurisez les ventes en ligne.** Il y a des risques associés aux transactions effectuées en ligne :

- Les données transmises peuvent être volées au moyen de virus informatiques.
- L'« usurpation de marques » (*brand spoofing*) fait référence à la technique qui consiste à se servir de l'identité d'entreprises pour créer des sites Web ou courriels bidons ressemblant à ceux d'organisations légitimes, afin de tromper les clients et les amener à fournir leurs renseignements personnels et financiers. On parle plus spécifiquement d'« hameçonnage » (*phishing*) lorsque ces attaques frauduleuses prennent la forme de courriels contrefaits.

---

Voici certaines des pratiques exemplaires pour lutter contre ces risques :

- Si vous demandez que le paiement soit fait par carte de crédit, minimisez les risques de fraude en utilisant le logiciel de cryptage recommandé par des spécialistes qui connaissent les meilleures technologies et appareils. Affichez sur votre site Web votre politique de confidentialité ainsi que les niveaux de cryptage et les autres caractéristiques de sécurité que vous utilisez.
- Informez vos clients des renseignements exacts que votre entreprise leur demandera, et de ceux qu'elle ne leur demandera pas, sur les sites Web ou par courriel.
- Fournissez aux clients les renseignements nécessaires pour qu'ils puissent se renseigner sur des courriels et des sites Web suspects ou les signaler.
- Assurez-vous que c'est bien vous la personne inscrite en tant que détentrice et responsable du site Web de votre entreprise, plutôt que le concepteur du site.
- Publicisez clairement les adresses valides du site Web de votre entreprise dans toutes vos communications.
- Enregistrez les variations des adresses du domaine de votre site Web pour éviter que d'autres les utilisent.

Le *Code canadien de pratiques pour la protection des consommateurs dans le commerce électronique*, disponible à [cmcweb.ca/commerceelectronique](http://cmcweb.ca/commerceelectronique), énonce les bonnes pratiques que pour les commerçants qui exercent des activités commerciales en ligne avec les consommateurs.

## Utilisation

**Limitez l'utilisation.** Les données ne devraient servir qu'aux fins déclarées ouvertement aux consommateurs.

**Limitez l'accès.** Après avoir fait l'inventaire des données que vous recueillez, déterminez qui devrait y avoir accès. Limitez l'accès aux personnes qui ont besoin de ces renseignements et protégez l'information par des mots de passe. Confiez exclusivement à votre gestionnaire de réseau la tâche de faire les copies de sauvegarde et les autres tâches qui exigent l'accès au réseau de votre entreprise. Bloquez l'accès

---

aux ordinateurs en veille avec des verrouillages automatiques qui demandent un mot de passe détenu par un utilisateur autorisé.

**Chiffrez vos données.** Les progiciels de cryptage autonomes sont compatibles avec diverses applications, et d'excellents logiciels sont disponibles sur le marché. Si un intrus réussit à traverser un pare-feu, les données du réseau peuvent demeurer en sécurité si elles sont chiffrées. Cryptez les ordinateurs portatifs et les autres périphériques utilisés à distance, comme les appareils sans fil (de type BlackBerry, par exemple). Faites la mise à jour de vos applications de cryptage. Vérifiez les accords des commerçants que votre entreprise a signés avec les émetteurs de cartes de paiement concernant les exigences en matière de cryptage. Dans la mesure du possible, évitez d'utiliser des ordinateurs communs et des numéros d'identification génériques ou de groupe pour l'ouverture de session.

**Les mots de passe sont essentiels.** Exigez que les employés utilisent une combinaison de lettres majuscules et minuscules, de chiffres et de symboles. Les mots de passe devraient être changés régulièrement (p. ex. tous les 90 jours).

**Faites des vérifications en ligne et hors ligne pour détecter les activités suspectes.** Presque tous les progiciels pare-feu, de cryptage et de création de mots de passe comportent une fonction de vérification qui enregistre les activités du réseau. Vérifiez les données sur les ouvertures de sessions et suivez les pistes de vérification en cas d'activité inhabituelle ou suspecte, comme l'accès par des employés à des données non reliées aux activités quotidiennes de l'entreprise.

## Divulgateion

**Sachez qui est votre interlocuteur.** Des escrocs reconnus coupables disent aux autorités combien il leur a été facile d'obtenir de précieux renseignements simplement en les demandant. Se faisant passer pour des fonctionnaires ou des représentants de sociétés de crédit, les voleurs fabriquent des histoires crédibles, téléphonent aux entreprises et obtiennent des employés qu'ils divulguent des renseignements habituellement conservés dans des classeurs verrouillés ou sur des disques durs protégés par un mot de passe.

**Autorisation.** Si votre organisation divulgue des renseignements personnels à des personnes autres que leur propriétaire, assurez-vous d'avoir l'autorisation légale requise. Rédigez des politiques strictes et claires expliquant aux employés comment et quand divulguer des renseignements.

**Les tiers.** Assurez-vous que les organisations avec lesquelles vous échangez des renseignements sur la clientèle (fournisseurs, entrepreneurs, clients, etc.) protègent les données qu'elles détiennent et que vous avez l'autorisation légale adéquate (c.-à-d. le consentement du client) pour échanger ces données avec elles.

**Faites preuve d'ouverture face à votre politique et à vos pratiques.**

Conformément à la législation sur la protection de la vie privée, vous êtes tenu de faire connaître votre politique et vos pratiques à quiconque en fait la demande. Informez les consommateurs des mesures en place dans votre organisation pour protéger leurs renseignements. Vous pouvez également leur suggérer de consulter la *Trousse d'information sur le vol d'identité des consommateurs* sur le site Web du comité des mesures en matière de consommation (CMC) fédéral, provincial et territorial à l'adresse [cmcweb.ca/volidentite](http://cmcweb.ca/volidentite).

## Sécurité et stockage des données

**Si vous stockez des données, assurez leur sécurité physique.**

- Les dossiers papier renfermant des renseignements personnels doivent être gardés sous clé et les ordinateurs, protégés par un mot de passe.
- Installez les serveurs dans un local sécuritaire à accès contrôlé et gardez sous clé les autres supports et périphériques (p. ex. les CD ou les bandes de sauvegarde).
- Gardez sous clé tous les ordinateurs portatifs pour empêcher que des voleurs s'en emparent.
- Empêchez les clients et le personnel non autorisé d'accéder aux zones privées et protégées.
- Donnez instruction aux employés de sauvegarder les données sur les lecteurs du réseau lorsqu'ils existent, et non sur le lecteur « C : » ou disque dur où elles sont moins en sécurité. En cas de vol du disque dur, les renseignements stockés sur les lecteurs du réseau restent protégés.
- Ne copiez pas des bases de données entières sur des appareils lorsqu'une liste partielle suffit.

- N'installez pas de modems ou de cartes de réseau local (LAN) dans les ordinateurs qui n'en ont pas besoin.
- Envisagez de faire installer un système d'alarme, de préférence un système relié à la centrale d'une entreprise de services de sécurité. L'assureur de votre entreprise peut sans doute vous aider à évaluer la sécurité de vos activités.
- Empêchez que des photocopies soient faites sans autorisation.

Lorsque vous mettez votre système à jour, mettez aussi à jour les processus de sécurité.\*

La compagnie d'assurance PME de l'Alberta a failli divulguer les données de nature délicate contenues dans des milliers de dossiers de clients, simplement en faisant la mise à jour que de quelques ordinateurs.

Certains renseignements personnels de nature délicate ont été à risque, notamment les noms, adresses, numéros de téléphone, numéros de dossier, détails des polices, revenus annuels et valeurs des maisons des assurés. Ces données, entre les mains de personnes mal intentionnées, auraient été suffisantes pour que des milliers de personnes puissent être victimes d'usurpation d'identité.

L'incident s'est produit lorsque la compagnie a vendu de vieux ordinateurs contenant toujours leurs disques durs à une petite entreprise qui achète, répare et revend de l'équipement informatique. Le revendeur a découvert un disque dur sur lequel était installé un système d'exploitation qui lui donnait accès, sans mot de passe, aux dossiers de la compagnie d'assurance. Si les bases de données étaient tombées entre les mains d'un pirate informatique, il aurait pu avoir accès aux dossiers des clients.

Heureusement, le revendeur était honnête et a immédiatement signalé l'erreur à la compagnie d'assurance.

La compagnie avait un logiciel permettant de vider complètement les disques durs de façon à ce qu'il n'y reste aucune donnée. Par contre, aucune procédure n'était en place pour que cette opération soit faite systématiquement. La compagnie a donc décidé qu'à l'avenir, lorsqu'elle devra se débarrasser de disques durs, elle les retirera des ordinateurs et les fera détruire.

*\* Toutes les anecdotes relatées dans les encadrés marginaux sont vraies. Seuls les noms, les lieux et d'autres détails mentionnés ont été changés.*

---

**Protection contre les virus.** Installez un logiciel antivirus sur tous les ordinateurs et scannez périodiquement les systèmes pour y déceler la présence de virus. Ne désactivez jamais le logiciel antivirus et mettez-le à jour fréquemment.

**Pare-feu.** Un pare-feu doit être installé à chaque point où un système informatique est en contact avec d'autres réseaux : accès à Internet, au système d'un client ou au réseau d'une compagnie de téléphone. Un pare-feu protège contre les accès non autorisés à de l'information. Demandez également à votre fournisseur de services Internet quels autres filtres peuvent être utilisés.

**Installez les correctifs de sécurité.** La plupart des fabricants de logiciel publient des mises à jour et des correctifs de sécurité pour corriger les bogues qui peuvent permettre aux pirates informatiques de s'introduire dans votre ordinateur. Vérifiez auprès du fabricant pour savoir s'il existe de nouveaux correctifs de sécurité ou s'il offre l'installation de ceux-ci avec fonctions automatisées.

## Élimination

**Sachez quels documents doivent être déchiquetés.** Lorsque vous recueillez des renseignements (sur papier ou sous format électronique) pour une transaction unique ou pour une utilisation temporaire, séparez-les des autres dossiers et détruisez-les ensuite de manière sécuritaire. Par exemple, les curriculum vitae de candidats non retenus peuvent contenir beaucoup de détails et devraient être déchiquetés. Les voleurs d'identité savent que les conteneurs de recyclage et les poubelles contiennent de précieux renseignements. Assurez-vous que les employés savent quels sont les documents de nature délicate à déchiqueter. Il est possible de recourir aux services d'une entreprise spécialisée dans la destruction de documents ou se procurer des déchiqueteurs à prix raisonnable. Les déchiqueteurs qui coupent les documents transversalement sont les plus efficaces.

**Destruction de données.** Établissez un calendrier pour la conservation des données basé sur des prescriptions légales, contractuelles, ou pour besoins de recours. Détruisez les données en conséquence, effacez les fichiers, supprimez les copies de toutes les bases de données et de tous les répertoires du réseau, et utilisez un logiciel de nettoyage pour vous assurer qu'elles sont supprimées à jamais. Le « nettoyage » réduit les risques qu'il reste des données dans le système. Lorsque vous vous débarrassez de matériel informatique, il est peut-être préférable de détruire physiquement le disque dur, les CD, les bandes et les disquettes, ou de faire appel à une entreprise spécialisée dans la destruction de ce genre d'objets.

## Le personnel et la sécurité des données

**Choisissez soigneusement vos employés.** Pour protéger votre entreprise contre la fraude interne, songez à vérifier les antécédents des personnes qui auront accès à des données de nature délicate. Il existe des entreprises qui peuvent faire ces vérifications (y compris le casier judiciaire, les références et les attestations d'études) pour vous. Faites régulièrement des vérifications de sécurité des employés qui travaillent dans des secteurs à risque élevé (p. ex. en même temps que l'évaluation annuelle du rendement des employés) afin de vous assurer que vos employés n'ont toujours pas de casier judiciaire.

**Donnez de la formation à vos employés.** Assurez-vous que votre personnel comprenne les politiques en matière de protection de la vie privée et la manière de demander aux clients leurs renseignements personnels. Affichez les règles suivantes comme liste de contrôle à l'intention de tous vos employés :

- Utilisez des mots de passe alphanumériques à l'ouverture d'une session et changez-les régulièrement.
- Ne demandez pas à un client de vous communiquer des données personnelles en présence de tiers et assurez-vous que le client peut entrer son NIP en toute confidentialité.
- Comparez les signatures et assurez-vous que le client est bien la personne qu'il dit être.
- Si vous constatez l'altération des terminaux ou des bases de données, signalez-le à la direction.
- Gardez sous clé les renseignements sur les clients.
- Déchiquez les rebuts renfermant des données à caractère confidentiel, y compris des informations sur les cartes de paiement et des photocopies de pièces d'identité.
- Ne laissez rien sur les bureaux le soir.
- Accédez aux bases de données uniquement lorsque vous en avez l'autorisation.
- Verrouillez les systèmes lorsqu'ils ne sont pas utilisés.

---

**Surveillez les menaces.** Chargez l'agent d'information ou un employé clé de faire le suivi des menaces potentielles à la sécurité et des mises à jour technologiques, et demandez-lui, le cas échéant, de les signaler aux employés et aux gestionnaires.

**Formation pour reconnaître des faux documents.** Formez vos employés sur la façon de reconnaître de fausses pièces d'identité.

**Accès au réseau.** Ne fournissez un accès au réseau qu'aux employés qui ont besoin d'obtenir des renseignements. Lorsqu'un employé quitte, annulez immédiatement leur accès au réseau.

## Modifiez vos pratiques

Les renseignements recueillis par votre entreprise changeront au fil du temps. Il en sera de même pour la technologie informatique, les bases de données et le personnel. Tenez compte des effets engendrés par tout changements dans vos activités sur la façon dont vous gérez les renseignements personnels détenus.

## 3. QUE FAIRE EN CAS D'INTRUSION

### Mesures à prendre lorsque les renseignements sont compromis

Mettez en place un plan d'action pour réagir en cas de vol ou de disparition de renseignements. Agir rapidement peut aider à réduire les dommages potentiels et éviter à votre organisation d'être tenue responsable dans une poursuite civile. Pour réagir à une intrusion, vous devez poursuivre deux pistes à la fois : mener une enquête interne, et élaborer un plan pour informer les personnes à l'extérieur de l'organisation qu'il y a eu une infraction à la sécurité.

### Enquêter sur l'incident

Vous devez comprendre ce qui s'est passé. Il vous faut donc déterminer :

- Quels renseignements ont été volés?
- Quand ont-ils été volés?
- Comment l'intrusion s'est-elle produite?
- Quels dossiers ont été touchés?
- Quelles mesures faut-il prendre pour vous assurer qu'aucune autre donnée n'est volée ou perdue?
- Y a-t-il lieu d'obtenir l'opinion de votre avocat et/ou comptable?

### Informer les clients et les organisations externes

Lorsqu'il y a intrusion, vous devez agir rapidement pour informer les clients touchés. Si vous ne gérez pas la situation de façon adéquate, les dommages causés à votre entreprise pourraient être énormes et permanents. Les délais sont critiques, parce que le fait d'avertir promptement les clients de l'intrusion peut aider à prévenir le vol d'identité ou à en limiter les conséquences. Personnalisez la lettre que vous enverrez

aux personnes concernées. Assurez-vous qu'elle est préparée sur le papier à en-tête de votre entreprise et signée par un représentant important. N'oubliez pas de mettre le logo ou le nom de l'entreprise sur l'enveloppe. Si le nombre d'individus affectés est restreint, avisez-les immédiatement. Si un grand nombre de personnes sont touchées (plus de 100), vous pourriez discuter de la façon la plus efficace d'informer les victimes potentielles en consultant d'abord les organisations suivantes :

Les agences d'évaluation du crédit du Canada :

Equifax (1-800-465-7166)

TransUnion Canada (1-877-525-3823); au Québec (1-877-713-3393)

Les Bureaux de crédit du Nord (1-800-532-8784)

Organismes policiers

Les personnes ou les entreprises touchées

Les Commissaires à la protection de la vie privée

**Agences d'évaluation du crédit.** Communiquez avec les spécialistes de la fraude à Equifax, TransUnion et, selon le cas, Les Bureaux de crédit du Nord, pour discuter du type d'avertissement et d'aide nécessaire pour veiller au traitement adéquat de la fraude. Les agences d'évaluation du crédit vous aideront à déterminer s'il y a lieu de lancer un avis de fraude.

Un avis de fraude indique aux créanciers de communiquer avec la personne touchée avant d'approuver un nouveau compte ou de modifier les comptes existants; ce qui peut être un outil efficace pour protéger vos clients contre le vol. Lors des discussions avec les agences d'évaluation du crédit, vous devriez demander un *numéro d'atteinte de sécurité de l'information*, et informer les clients touchés d'utiliser ce *numéro* lors de toutes leurs communications avec les ARC.

**Organismes policiers.** Vous devriez téléphoner au service de police locale pour les informer de l'intrusion et, si on vous le recommande, déposer un rapport de vol. Vous devez également signaler l'intrusion au centre d'appel national PhoneBusters, le centre d'appel antifraude du Canada ([phonebusters.com](http://phonebusters.com) ou 1-888-495-8501) ou faire un rapport électronique sur le site Web de la GRC pour signaler les crimes économiques, [RECOL.ca](http://RECOL.ca).

**Personnes et entreprises touchées.** Déterminez comment informer les personnes touchées par l'intrusion. Vous devez les informer de la nature de l'incident, du type de renseignements volés, de la probabilité qu'ils soient utilisés à mauvais escient et des conséquences éventuelles du vol d'identité. Donnez-leur les renseignements nécessaires

---

pour communiquer avec la personne-ressource au sein de votre organisation, avec les agences d'évaluation du crédit et, au besoin, avec la police. Donnez-leur également les renseignements à jour sur le vol d'identité. Le site Web du CMC, à [cmcweb.ca/volidentite](http://cmcweb.ca/volidentite), contient des renseignements pour aider les gens à se protéger contre le vol d'identité et sur ce qu'il faut faire s'il se produit.

**Commissaires à la protection de la vie privée.** Indépendant du gouvernement, le commissaire fédéral cherche à promouvoir la protection des renseignements personnels et s'assure du respect de la LPRPDE. Communiquez avec le bureau du commissaire pour obtenir des conseils sur les questions touchant la protection de la vie privée en cas d'intrusion. Veuillez noter que le Québec, la Colombie-Britannique et l'Alberta ont des lois distinctes sur la protection des renseignements personnels qui sont très similaires à la LPRPDE. Par conséquent, si vous exploitez votre entreprise dans l'une de ces provinces, veuillez communiquer avec le commissaire provincial compétent. Vous pouvez joindre le commissaire fédéral au 1-800-282-1376 ou à [privcom.gc.ca](http://privcom.gc.ca) sur lequel vous trouverez également des liens vers les commissaires des provinces).

## Communiquer avec les médias

Selon la nature de l'intrusion et le nombre de personnes touchées, il est possible que vous deviez répondre à des appels des médias. Il serait judicieux de préparer une réponse à l'intention des médias en même temps que vous rédigez les lettres destinées aux personnes touchées. Soyez franc et mettez l'accent sur les mesures que vous prenez pour régler le problème. Diffuser de l'information dans les médias peut permettre de faire peur au voleur et l'empêcher d'utiliser les renseignements dérobés parce qu'il comprendra que les agences d'évaluation du crédit et la police attendent qu'il utilise les données.

***Vous connaissez vos clients.***

***Pourquoi laisser un voleur d'identité vous les dérober?***

## 4. OUTILS : INFORMER LES CLIENTS DU VOL DE RENSEIGNEMENTS PERSONNELS

### MODÈLE DE LETTRE DE NOTIFICATION

Date\_\_\_\_\_

Madame, Monsieur\_\_\_\_\_,

Nous regrettons de devoir vous informer d'un incident qui peut avoir compromis la sécurité d'une base de données renfermant certains de vos renseignements personnels. Nous nous excusons des incon vénients que cet incident pourrait vous causer.

*[Décrire la façon dont les renseignements sont compromis et ce que vous faites à cet égard.]*

Les principales agences d'évaluation du crédit du Canada, Equifax et TransUnion, ont été informées de cette intrusion et ont fourni le numéro d'atteinte de sécurité de l'information suivant : XXXXX. Vous devrez fournir ce numéro lors de toute communication avec elles. Equifax et TransUnion recommandent que vous téléphoniez à leurs agents pour déterminer si un avis de fraude doit être inscrite dans votre dossier de crédit et pour discuter des autres mesures à prendre (Equifax : 1-800-465-7166 et TransUnion : 1-877-525-3823).

Un avis de fraude indique aux créanciers de communiquer avec vous avant d'accorder du crédit, d'ouvrir un compte ou de modifier vos comptes existants. Vous devez par contre savoir que même si la plupart des créanciers vous téléphoneront, la loi ne les oblige pas à le faire; par conséquent, cette protection n'est pas sans faille.

Signalez, dès que vous en avez connaissance, toute activité non autorisée à votre institution financière, aux agences d'évaluation du crédit, aux organismes policiers et au centre d'appel national PhoneBusters (unité de police antifraude nationale, 1-888-495-8501).

Un rapport de police a été préparé; le numéro du rapport est YYYYY. Votre institution financière ou vos autres créanciers pourraient exiger le rapport de police pour effacer les frais frauduleux.

Vous pouvez également demander aux agences d'évaluation du crédit de vous envoyer gratuitement une copie de votre dossier de crédit en fournissant les preuves d'identification appropriées. Visitez leurs sites Web pour obtenir des plus amples renseignements sur les preuves d'identification acceptées. Si vous recevez une copie de votre dossier et n'y relevez aucune activité non autorisée, il est tout de même recommandé que vous vérifiiez vos dossiers de crédit périodiquement.

Nous vous recommandons de prendre ces précautions afin de réduire les risques de pertes financières ou les risques que vos renseignements soient utilisés à des fins illicites.

Nous vous recommandons également de consulter le site [cmcweb.ca/volidentite](http://cmcweb.ca/volidentite) pour obtenir des renseignements sur le vol d'identité, notamment :

- Conseils pour réduire les risques de vol d'identité;
- Que faire si cela vous arrive;
- la Déclaration de vol d'identité;
- les Questions souvent posées;
- la Liste de vérification concernant le vol d'identité des consommateurs.

Si vous avez des questions, vous pouvez communiquer avec *[nom de la personne chargée du dossier relatif à l'intrusion]*, agent d'information de notre entreprise, au *[numéro de téléphone et adresse s'il y a lieu]* .

Une fois de plus, nous regrettons tout inconfort que cet incident peut vous causer.

# Que dire et comment réagir en cas d'intrusion?

## Questions et réponses types

Si les renseignements d'une personne sont perdus ou volés, celle-ci aura des questions à vous poser. Préparez vos employés à répondre à toute personne concernée par un tel problème, que ce soit des clients, des fournisseurs et des partenaires, ou à toute autre organisation liée à votre entreprise. **Soyez spécifique et agissez rapidement.**

Question : Quels sont mes renseignements personnels qui ont été perdus?

Réponse : Vous devrez informer les victimes potentielles des données qui ont été perdues afin d'empêcher ou de réparer d'éventuels préjudices.

Question : Pourquoi disposiez-vous de ces renseignements personnels au départ?

Réponse : Conformément aux lois sur la vie privée, les organisations doivent déterminer les fins pour lesquelles elles recueillent les renseignements personnels, et ce, au moment de la collecte ou au préalable. Vous devriez également vous préparer à expliquer pourquoi il était nécessaire de stocker ces renseignements.

Question : Quand ces données ont-elles été perdues?

Réponse : Si une victime signale un vol possible, la séquence des faits est importante, car les émetteurs de crédit doivent savoir quand les frais frauduleux pourraient survenir.

Question : Comment cet incident s'est-il produit?

Réponse : Les personnes concernées exigeront une réponse de votre part. Plus vous aurez pris de mesures pour éviter une intrusion et plus ces mesures de prévention et de gestion seront sécuritaires, plus vous serez à l'aise pour répondre à cette question.

---

Question : Que faites-vous pour régler le problème?

Réponse : Vous devez préparer une réponse prudente, qui comprendra les mesures correctives que vous avez prises.

Question : Que peut faire un voleur d'identité avec mes renseignements?

Réponse : Cela dépendra de la nature des données qui sont concernées. À partir de renseignements personnels, voici quelques-unes des formes courantes de fraude : frais frauduleux apparaissant sur des cartes de crédit ou des comptes bancaires existants, ouverture de nouveaux comptes de crédit sous un autre nom, mise en service d'un téléphone cellulaire ou ouverture d'autres comptes sous un autre nom.

Question : Comment puis-je me protéger maintenant que l'incident a eu lieu?

Réponse : Indiquez aux victimes potentielles de communiquer avec les agences d'évaluation du crédit et les institutions financières, de réclamer un avis de fraude, et de vérifier leurs dossier de crédit au moins une fois par année.

Question : Si on place un avis de fraude dans mon dossier, cela garantit-il qu'aucun crédit ne sera accordé sans que je sois contacté en premier?

Réponse : Il faut informer le client que même si la plupart des créanciers téléphoneront, la loi ne les oblige pas à le faire; par conséquent, cette protection n'est pas sans faille.