



# Vol d'identité

## TROUSSE D'INFORMATION SUR LE VOL D'IDENTITÉ DES CONSOMMATEURS

### **VOL D'IDENTITÉ:** **Identifiez-le.** **Signalez-le.** **Enrayez-le.**

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

PHONE **BUSTERS**

Le centre d'appel antifraude du Canada

Canada



Québec

NOVA SCOTIA

New Brunswick  
CANADA

Manitoba



BRITISH  
COLUMBIA

Prince  
Edward  
Island



Government of  
Saskatchewan

Alberta  
Government

Newfoundland  
Labrador

Yukon  
Government

Northwest  
Territories

Nunavut

## Vol d'identité : En êtes-vous victime?

---

### Qu'est-ce que le vol d'identité?

Le vol d'identité se produit lorsque quelqu'un se sert de vos renseignements personnels à votre insu ou sans votre consentement pour commettre un crime, comme la fraude, le vol ou la contrefaçon.

### En quoi consistent les renseignements personnels?

Tout renseignement précis ou subjectif, consigné ou non, au sujet d'un particulier identifiable est un renseignement personnel. Il peut s'agir de vos nom, adresse, âge, sexe, numéros d'identification et de cartes de crédit, revenu, emploi, actif, obligations, relevés de paiements, références personnelles et dossier médical.

Il peut s'agir également de renseignements au sujet de vos préférences d'achat, de votre famille (comme le nom de jeune fille de votre mère), de vos intérêts ou de vos attitudes.

En général, les données recueillies à votre sujet par les entreprises ou votre employeur ne doivent être utilisées qu'aux fins pour lesquelles elles ont été recueillies, ou à une autre fin pour laquelle vous avez donné votre consentement. Les lois sur les renseignements personnels exigent que le gouvernement et les entreprises mettent en place des systèmes faisant en sorte que les renseignements personnels de leur clientèle soient protégés, exacts, recueillis avec son consentement et utilisés uniquement aux fins stipulées.

La *Loi sur la protection des renseignements personnels et les documents électroniques* (LPRPDÉ) du gouvernement fédéral et les lois provinciales équivalentes de la Colombie-Britannique, de l'Alberta et du Québec s'appliquent aux entreprises qui recueillent vos renseignements personnels et vous donnent le droit de consulter et de demander d'apporter des corrections à tout renseignement qu'une entreprise aurait pu recueillir à votre sujet. Pour obtenir plus d'information relative à vos droits en vertu de la LPRPDÉ, veuillez télécharger " Vos droits en matière de vie privée : un guide à l'intention des particuliers " du Commissariat à la protection de la vie privée du Canada à l'adresse [www.privcom.gc.ca](http://www.privcom.gc.ca). Vous y trouverez également de l'information relative aux diverses lois provinciales.

### Pourquoi devriez-vous vous préoccuper du vol d'identité?

Les voleurs d'identité s'emparent de certains renseignements personnels importants et s'en servent pour usurper votre identité et commettre des crimes en votre nom. Si vous en êtes victime, vous pourriez devoir passer de nombreuses heures à tenter de rectifier la situation et vivre des moments d'angoisse tout au long du processus. Dans les cas extrêmes, votre réputation pourrait être entachée, puisque les jugements de la cour en matière d'insolvabilité peuvent paraître dans votre dossier et votre cote de crédit pourrait en souffrir. Conséquemment, vous pourriez avoir de la difficulté à vous trouver un emploi et à obtenir du crédit en temps opportun.

### Indices que votre identité pourrait avoir été volée

- Une banque ou une société émettrice de carte de crédit communique avec vous au sujet de transactions douteuses

- Des factures et des relevés bancaires ou de carte de crédit arrivent en retard ou pas du tout (quelqu'un pourrait avoir fait acheminer votre courrier à une autre adresse)
- Un créancier ou une agence de recouvrement communique avec vous au sujet de dettes que vous n'avez pas contractées
- Des achats et / ou des retraits que vous n'avez pas effectués apparaissent sur vos factures mensuelles ou vos relevés bancaires
- On vous refuse du crédit pour des raisons qui ne correspondent pas à votre connaissance de votre situation financière
- Votre dossier de crédit indique un crédit accordé que vous n'avez pas demandé
- Votre propriété est grevée d'un privilège dont vous ignoriez l'existence
- Vous recevez des factures pour des comptes qui ne vous appartiennent pas

## **Façons dont les voleurs d'identité vous dérobent vos renseignements personnels**

- Ils volent votre courrier dans votre boîte à lettres ou bac de recyclage, ou réorientent frauduleusement votre courrier en contrefaisant votre signature sur un formulaire de " changement d'adresse ".
- Ils s'emparent de vos renseignements personnels et particuliers dans les sacs à main et les portefeuilles perdus ou volés à votre domicile, dans votre véhicule ou votre ordinateur.
- Ils volent des renseignements personnels récupérés dans des dispositifs électroniques personnels perdus ou volés comme des assistants numériques, des lecteurs audionumériques, des téléphones cellulaires et des ordinateurs portatifs.
- Ils prétendent être un représentant digne de confiance d'une entreprise ou un agent d'application de la loi, en personne ou en ligne, et vous demandent vos renseignements personnels comme votre dossier de crédit ou le mot de passe de votre compte bancaire.
- Ils altèrent les guichets automatiques bancaires (GAB) et terminaux de points de vente, de telle sorte que votre numéro de carte de débit ou de crédit et votre numéro d'identification personnel (NIP) puissent être enregistrés.
- Ils se procurent les renseignements au sein même d'organismes, par exemple auprès d'employés qui acceptent des pots-de-vin ou qui volent vos renseignements personnels pour d'autres. Les organismes peuvent également divulguer à leur insu vos renseignements personnels à des criminels qui prétendent représenter des entreprises honnêtes.
- Ils consultent les sources publiques, comme les journaux (notices nécrologiques), les annuaires téléphoniques et les registres du domaine public (certifications professionnelles).
- Ils se servent de " faux " courriels et de sites Web frauduleux (usurpation de marque ou usurpation d'identité d'entreprise) pour tromper les clients et les mener à divulguer leurs renseignements personnels et financiers selon une pratique appelée l'" hameçonnage ".
- Ils utilisent des logiciels espions pour recueillir des données se trouvant dans votre ordinateur.

# Gare à votre identité : Conseils pour réduire les risques du vol d'identité

---

La prévention du vol d'identité est une responsabilité qu'un consommateur et les entités qui détiennent ses renseignements personnels et financiers se partagent. Les consommateurs tout comme les entreprises doivent prendre les mesures pour protéger leurs données. Même si vous n'êtes pas capable d'enrayer complètement le vol d'identité, voici des mesures importantes qui peuvent être prises pour en réduire le risque.

## Protégez vos renseignements et vos documents personnels

- Ne conservez sur vous que les pièces d'identification dont vous avez besoin. Conservez sous-clé et en lieu sûr toutes vos autres pièces d'identification (c.-à-d. NAS, certificat de naissance, passeport).
- Soyez prudent lorsque vous divulguez des renseignements personnels et n'en fournissez pas plus qu'il est nécessaire. Si quelqu'un vous demande des renseignements qui ne sont pas pertinents à la transaction que vous faites, demandez-en la raison.
- Lorsque vous divulguez des renseignements personnels et financiers faites-le discrètement et dissimulez votre NIP lorsque vous utilisez votre carte de débit. Il est à noter que les consommateurs ont certains droits et certaines responsabilités en vertu du Code de pratique Canadien des services de cartes de débit. Pour obtenir davantage d'information, veuillez communiquer avec l'Agence de la consommation en matière financière du Canada ([www.fcac-acfc.gc.ca](http://www.fcac-acfc.gc.ca)).
- Renseignez-vous au sujet de la protection de vos renseignements personnels au travail et auprès des entreprises et des œuvres de bienfaisance.
- Ne laissez pas traîner vos renseignements personnels à la maison, dans votre véhicule ou au bureau. N'inscrivez pas plus que votre nom et votre adresse sur vos chèques personnels.
- Verrouillez votre boîte à lettres à la maison, si possible. Si vous prévoyez vous absenter, demandez à un voisin digne de confiance de ramasser votre courrier. Vous pouvez aussi vous rendre au bureau de poste de votre quartier (avec une pièce d'identification) et demandez à Postes Canada de retenir votre courrier. Ce service comporte des frais.
- Ne divulguez jamais de renseignements personnels au téléphone, sur Internet ni par la poste à moins d'avoir établi vous-même le contact et de connaître très bien l'entreprise. Les voleurs d'identité peuvent se servir d'offres " bidons " ou prétendre représenter une institution financière, un fournisseur de services Internet ou même un organisme gouvernemental pour vous amener à divulguer des renseignements permettant de vous identifier.
- Déchiquetez ou détruisez les documents contenant des renseignements personnels de nature délicate avant de les jeter à la poubelle ou au bac de recyclage. Vous aiderez ainsi à faire échec aux pêcheurs de poubelles à la recherche de relevés de transactions, de copies de demandes de crédit, de formulaires d'assurance, de chèques, de relevés bancaires et de vieilles déclarations de revenus. Coupez les cartes de crédit et de débit expirées ou inutilisées. La carte pourrait être expirée, mais le numéro pourrait être encore valide et servir à faire des achats.

## Soyez vigilant

### Portez attention aux détails financiers

Le fait de porter attention aux détails financiers pourrait vous aider à reconnaître les indices que vous êtes peut-être victime d'un vol d'identité.

- Lorsque vous utilisez votre carte bancaire ou de débit pour retirer de l'argent ou pour faire un achat, protégez l'entrée de votre NIP. Ne confiez jamais votre NIP à quiconque même pas à une personne qui affirme être agent de police ou employé d'une banque. Choisissez un NIP difficile à deviner, puisque vous pourriez être tenu responsable si vous utilisez un NIP composé de votre nom, de votre numéro de téléphone, de votre date de naissance, de votre adresse ou de votre numéro d'assurance sociale (NAS). Rappelez-vous qu'aucun représentant d'une institution financière ou de la police ne vous demandera votre NIP.
- Conservez vos relevés d'opérations de carte de crédit, de carte de débit et guichet automatique bancaire (GAB) de telle sorte à pouvoir les comparer à vos relevés de compte. Si vous décidez de vous débarrasser de vos relevés d'opérations ou de compte, déchiquetez-les ou détruisez-les, ne le faites pas dans un lieu public.
- Signalez immédiatement à votre institution financière tout écart apparaissant sur vos relevés, qu'il s'agisse d'opérations que n'avez pas effectuées ou d'opérations que vous avez faites, mais qui n'y apparaissent pas.
- Notez la date de paiement de votre carte de crédit, de vos factures de services publics et de vos relevés bancaires. Si vous ne les recevez pas à la date habituelle, appelez l'institution financière ou la société qui vous offre les services publics - un voleur d'identité pourrait avoir changé l'adresse de facturation. Si vous ne recevez pas le courrier de plus d'une entreprise, communiquez avec le bureau de poste pour indiquer que vous soupçonnez que votre courrier a été réorienté à votre insu.
- Portez attention aux dates d'expiration des cartes de crédit. Si vous n'avez pas reçu votre carte de remplacement, communiquez avec la société émettrice. Quelqu'un peut l'avoir prise dans votre boîte à lettres ou avoir changé l'adresse postale.
- Conservez en lieu sûr une liste des noms, numéros de compte et dates d'expiration de vos cartes. Elle pourrait vous servir au moment d'aviser vos créanciers de la perte ou du vol d'une carte.

### Vérifiez votre dossier de crédit

Une fois l'an, ou si vous soupçonnez que vos renseignements personnels ont été volés, obtenez une copie de votre dossier de crédit auprès de chacune des agences importantes d'évaluation du crédit (bureaux de crédit). Le dossier vous indique les renseignements que l'agence conserve au sujet de vos antécédents en matière de crédit, de vos renseignements financiers, des jugements et de toute activité de recouvrement dont vous pourriez faire l'objet. Il y est également indiqué qui a fait la demande de renseignements à votre sujet. Vous pouvez obtenir une copie de votre dossier de crédit (une copie par année) de l'une des agences suivantes gratuitement par la poste ou en ligne, moyennant certains frais :

Equifax Canada : [www.equifax.ca](http://www.equifax.ca) (1-866-779-6440)

Trans Union Canada : [www.tuc.ca](http://www.tuc.ca) (1-877-525-3823, au Québec 1-877-713-3393)

Northern Credit Bureau : [www.creditbureau.ca](http://www.creditbureau.ca) (1-800-532-8784)

En vérifiant, vous pouvez repérer des dettes qui ne sont pas les vôtres et savoir qui a demandé des renseignements à votre sujet. Vous devez assurer le suivi si un prêteur ou une société

émettrice de carte de crédit a fait une demande de renseignements et que vous n'avez pas de compte chez eux ou que vous n'avez pas fait de demande de crédit ou de carte chez eux. Quelqu'un d'autre peut avoir utilisé votre nom.

Pour obtenir plus d'information afin de comprendre ce qu'est un dossier de crédit, jetez un coup d'œil à Comprendre votre dossier de crédit et votre pointage de crédit, disponible sur le site de l'Agence de la consommation en matière financière du Canada ([www.fcac-acfc.gc.ca](http://www.fcac-acfc.gc.ca)).

## **Protégez votre ordinateur et les données qu'il renferme**

Le clavardage, le magasinage et les opérations bancaires en ligne sont très pratiques dans notre vie quotidienne, mais si vous ne protégez pas votre ordinateur de façon appropriée, vos renseignements personnels et financiers peuvent être à risque.

Une façon courante pour les pirates de voler des renseignements personnels consiste à utiliser des logiciels espions qui recueillent les données de l'utilisateur au moyen de sa connexion Internet à son insu. Les logiciels espions sont généralement dissimulés dans des gratuits (freewares) ou des partagiciels (sharewares) (comme des logiciels de téléchargement de musique et de vidéos ou de jeux en ligne) qui peuvent être téléchargés d'Internet. Une fois installé, le logiciel espion surveille l'activité de l'utilisateur sur Internet et transmet cette information en arrière-plan à quelqu'un d'autre. Le logiciel espion peut également recueillir des adresses électroniques et même des mots de passe et des numéros de carte de crédit.

Les mesures suivantes peuvent vous aider à vous protéger contre le vol d'identité lorsque vous êtes en ligne :

- Créez toujours des mots de passe composés de lettres (majuscules et minuscules), de chiffres et de symboles. N'utilisez pas les fonctions d'ouverture de session automatiques pour sauvegarder votre nom d'utilisateur et votre mot de passe.
- Installez un pare-feu, un anti-virus, un anti-logiciel espion et un logiciel de sécurité, et faites-en régulièrement la mise à jour.
- Ne transmettez pas de renseignements personnels ou confidentiels par courriel. Les messages courriels NE sont PAS sécuritaires.
- N'essayez pas, n'achetez pas et ne répondez pas aux pourriels (courriels non sollicités) ou aux courriels hameçons qui demandent des renseignements personnels ou financiers. Les pourriels ou les courriels hameçons sont souvent la source d'escroqueries, de virus et de contenu offensant. Supprimez-les!
- Installez des retouches de sécurité dans votre système d'exploitation et faites-en la mise à jour régulièrement et fréquemment. La plupart des fabricants de logiciels publient régulièrement des mises à jour et des retouches de leurs logiciels pour corriger les bogues qui pourraient permettre aux intrus d'attaquer votre ordinateur. Toutefois, c'est à vous de vous renseigner.
- Soyez à l'affût de toute activité suspecte en ligne. Presque tous les pare-feu et programmes de chiffrement renferment des fonctions de vérification qui enregistrent les activités sur le réseau. Consultez les pistes de vérification afin d'y repérer toute activité anormale ou suspecte, p. ex. l'utilisation de fichiers informatiques utilisés à votre insu.
- Lorsque vous vous débarrassez, vendez ou donnez votre matériel informatique, assurez-vous de détruire de façon permanente les renseignements personnels qui se trouvent sur le disque dur. Si vous vous en débarrassez, vous pouvez le détruire physiquement; autrement, utilisez des logiciels d'écrasement par réécriture. Renseignez-vous à ce sujet.

- Si vous utilisez un ordinateur portable, verrouillez-le physiquement pour éviter que les voleurs de s'en emparent et, par le fait même, qu'ils dérobent les renseignements personnels qu'il contient.

### **Ne magasinez et ne faites vos opérations financières que chez des marchands dignes de confiance**

- Assurez-vous que le site Web est légitime. Les fraudeurs peuvent créer un faux site Web (usurpation de marque ou usurpation d'identité d'entreprise) dans le but de tromper les consommateurs et de les amener à divulguer des renseignements personnels ou financiers. Assurez-vous que l'adresse URL est exacte - y compris le domaine (.com, .ca, etc.)
- Avant d'indiquer tout renseignement personnel sur un site Web, consultez-en la politique en matière de protection de renseignements personnels pour savoir à quelles fins ceux-ci pourraient être utilisés.
- Avant de fournir le numéro de votre carte de crédit ou d'autres renseignements financiers à une entreprise, assurez-vous que le marchand se sert d'un système transactionnel sécuritaire. La plupart des logiciels de navigation indiquent lorsque vous utilisez un lien Internet sécuritaire. Pour savoir si un site Web est sécuritaire, assurez-vous que son adresse commence par https://, l'icône d'un cadenas verrouillé ou d'une clé intacte dans le coin inférieur droit de l'écran devrait également apparaître.
- Après avoir effectué une opération financière ou bancaire en ligne, assurez-vous de mettre fin à la session et de vider la mémoire cache et le fichier de témoins (cookies). La plupart des institutions financières fournissent des instructions sur la façon de procéder sous leur rubrique ayant trait à la sécurité.
- Si vous recevez un courriel non-sollicité vous demandant des renseignements personnels ou financiers, n'y répondez pas. On cherche à vous faire mordre à l'hameçon. Certains fraudeurs envoient des courriels en prétendant représenter une entreprise ou une banque avec laquelle vous faites affaire habituellement, quelquefois même, ils vous orientent vers un site Web identique à celui de l'entreprise ou de la banque, mais il s'agit en fait d'un site frauduleux. Les représentants d'entreprises dignes de confiance ne vous demanderont jamais de fournir des renseignements personnels ou financiers de cette façon. Il est à noter que des tentatives de vol d'identité semblables peuvent se faire par téléphone (une pratique appelée parfois l'hameçonnage vocal). Lorsque vous recevez un appel d'une personne prétendant représenter votre institution financière et que vous avez des doutes, raccrochez, et confirmer en composant le numéro de téléphone qui apparaît sur votre relevé bancaire et non pas celui que vous a fourni la personne qui vient de vous appeler.

### **Dispositifs électroniques personnels**

Tout dispositif électronique contenant des renseignements personnels peut être utilisé pour dérober vos renseignements si un voleur s'en empare. Les assistants numériques, les lecteurs audionumériques, les téléphones cellulaires et les ordinateurs portatifs peuvent servir tous à entreposer des renseignements personnels. Afin de protéger vos renseignements, essayez de créer des mots de passe lorsque vous pouvez le faire. La plupart des dispositifs offrent la possibilité de les " verrouiller " de telle sorte que les données ne soient accessibles qu'au moyen d'un mot de passe. De plus, lorsque vous transportez un dispositif électronique, faites-le de telle sorte à éviter de l'échapper ou de l'oublier quelque part par mégarde. Si vous prévoyez vendre, donner ou vous débarrasser d'un dispositif électronique, assurez-vous de prendre les mesures appropriées pour effacer tous vos renseignements personnels du dispositif. La plupart des fabricants peuvent vous indiquer la façon de procéder.

## Conservez vos documents clés en lieu sûr

Ne conservez sur vous que les pièces d'identification dont vous avez besoin. Si vous conduisez, vous aurez besoin bien sûr de votre permis de conduire, et ce serait une bonne idée de conserver également sur vous votre carte santé provinciale ou territoriale. Toutefois, votre certificat de naissance, votre carte d'assurance sociale (NAS), votre passeport et votre carte de citoyenneté devraient être gardés sous clé, à moins que vous en ayez besoin dans un but particulier. Si de tels documents sont volés, ils peuvent servir à commettre un crime ou à usurper votre identité, ce qui pourrait avoir de graves conséquences. Si vous devez conserver sur vous une carte d'identification importante, gardez-en une photocopie en lieu sûr.

Types de documents à protéger :

- Certificat de naissance
- Numéro d'assurance sociale
- Passeport

Notez que votre numéro d'assurance sociale (NAS) est un numéro confidentiel qui n'est requis, par la loi, que pour déclarer des revenus lorsqu'une personne les tire d'un emploi ou d'un investissement. Même si de nombreuses entreprises peuvent vous demander votre NAS à d'autres fins, vous avez le droit de refuser dans de telles circonstances. Pour obtenir plus d'information, veuillez visiter le site du Commissariat à la protection de la vie privée du Canada à [www.privcom.gc.ca](http://www.privcom.gc.ca).

# Vol d'identité : Que faire si cela vous arrive

---

## Signalez-le!

Si vous êtes victime de vol d'identité, il y a des mesures à prendre pour réduire les dommages et aider à prévenir d'autres fraudes ou vols. Aussitôt que vous découvrez la fraude ou le vol, suivez les étapes suivantes pour en faire le signalement.

- Appelez vos institutions financières - demandez à leurs représentants d'annuler vos cartes et de vous en émettre de nouvelles. Si vous ne signalez pas immédiatement la perte ou le vol d'une carte vous pourriez être tenu responsable de toute perte financière en découlant.
- Communiquez avec la police locale. Si un rapport est produit, assurez-vous d'inclure le numéro du rapport de police que l'on vous aura attribué dans toute la correspondance relative à ce vol.
- Communiquez avec les principales agences canadiennes d'évaluation de crédit :  
Trans Union du Canada à [www.tuc.ca](http://www.tuc.ca) (1-866-525-0262, au Québec 1-877-713-3393)  
Equifax Canada à [www.equifax.ca](http://www.equifax.ca) (1-866-779-6440)  
Les Bureaux de crédit du nord Inc. à [www.creditbureau.ca](http://www.creditbureau.ca) (1-800-532-8784)  
Demandez à chaque agence de vous envoyer une copie de votre dossier de crédit, et demandez si une note indiquant la fraude devrait être versée à votre dossier.
- Remplacez vos cartes d'identification comme votre carte de santé, votre permis de conduire ou votre NAS en appelant 1 800 O-Canada. Un agent pourra vous orienter vers l'organisme fédéral, provincial ou territorial approprié pour que vos cartes soient remplacées.
- Si votre courrier disparaît, communiquez avec Postes Canada à [www.postescanada.ca](http://www.postescanada.ca) (1-800-267-1177).
- Communiquez avec chaque organisme qui a fourni du crédit non autorisé, de l'argent, de l'information, des biens ou des services au voleur qui s'est emparé de votre identité, et demandez à leurs représentants de faire enquête sur l'incident et d'annuler toutes les cartes qui auraient été touchées et de fermer tous les comptes frauduleux.  
Renseignez-vous au sujet des points suivants :  
De quels renseignements l'entreprise a-t-elle besoin pour faire enquête?  
L'entreprise a-t-elle amorcé une enquête criminelle? Si tel est le cas, quel est le numéro du rapport de police?  
Que devez-vous faire pour que vos pertes vous soient remboursées?
- Pour obtenir des conseils au sujet de la protection des renseignements personnels et des questions ayant trait au vol d'identité (LPRPDÉ), communiquez avec le Commissariat à la protection de la vie privée du Canada (1-800-282-1376 ou [www.privcom.gc.ca](http://www.privcom.gc.ca)). Il est à noter que le Québec, la Colombie-Britannique et l'Alberta disposent de leur propre loi de protection des renseignements personnels, semblable à la LPRPDÉ. Alors si vous êtes résident de l'une de ces provinces, communiquez avec le commissaire provincial correspondant.
- Pour aider à combattre la fraude, assurez-vous de signaler l'incident à Phonebusters, le centre d'appels antifraude du Canada. Phonebusters recueille l'information et les renseignements relatifs au vol d'identité et fournit des conseils et de l'aide aux victimes [www.phonbusters.com](http://www.phonbusters.com) (1-888-495-8501).

## Prenez des notes

Assurez-vous de noter les étapes que vous avez suivies pour signaler l'utilisation frauduleuse de votre identité. Servez-vous du tableau suivant pour vous aider, assurez-vous de le conserver en lieu sûr afin de pouvoir le consulter.

Banques, sociétés émettrices de carte de crédit et autres entreprises				
Entreprise	Adresse et numéro de téléphone	Date du contact	Personne-ressource	Commentaires

Agences d'évaluation du crédit				
Agence	Numéro de téléphone	Date du contact	Personne-ressource	Commentaires
Equifax Canada	1-866-779-6440			
Trans Union Canada	1-877-525-3823			
Trans Union Canada - résidents du Québec	1-877-713-3393			
Credit du Nord	1-800-465-7166			

Application de la loi					
Agence	Numéro de téléphone	Date du contact	Personne-ressource	Numéro du dossier, si disponible	Commentaires
Police locale					
Phonebusters	1-888-495-8501				

## Personnes-ressources clés du gouvernement

Si vous avez perdu des documents émis par le gouvernement ou qu'ils vous ont été volés, il est important de le signaler immédiatement de telle sorte qu'ils soient annulés et que vous puissiez faire une nouvelle demande pour les remplacer.

Tel que déjà mentionné, pour remplacer des documents importants, veuillez communiquer avec le gouvernement du Canada au **1 800 O-Canada** (1-800-622-6232 ATME 1-800-465-7735). On vous orientera vers l'organisme approprié. Même si les agents du **1 800 O-Canada** peuvent vous orienter vers votre gouvernement provincial ou territorial en vue d'obtenir des documents clés émis par les gouvernements provinciaux et territoriaux, vous pouvez aussi communiquer avec eux directement au moyen des coordonnées suivantes :

<b>Terre-Neuve-et-Labrador</b> Téléphone : (709) 729-2600 Site Web : <a href="http://www.gov.nl.ca">www.gov.nl.ca</a>	<b>Nouvelle-Écosse</b> Sans frais : 1-800-670-4357 Site Web : <a href="http://www.gov.ns.ca">www.gov.ns.ca</a>	<b>Île-du Prince-Édouard</b> Téléphone : (902) 368-4000 Site Web : <a href="http://www.gov.pe.ca">www.gov.pe.ca</a>
<b>Nouveau Brunswick</b> Sans frais : 1-888-762-8600 Site Web : <a href="http://www.snb.ca">www.snb.ca</a>	<b>Québec</b> Sans frais : 1-800-363-1363 Site Web : <a href="http://www.gouv.qc.ca">www.gouv.qc.ca</a>	<b>Ontario</b> Sans frais : 1-800-267-8097 ATME sans frais : 1-800-268-7095 Site Web : <a href="http://www.gov.on.ca">www.gov.on.ca</a>
<b>Manitoba</b> Sans frais : 1-866-626-4862 ATME : 204-945-4796 Site Web : <a href="http://www.gov.mb.ca">www.gov.mb.ca</a>	<b>Saskatchewan</b> Site Web : <a href="http://www.gov.sk.ca">www.gov.sk.ca</a>	<b>Alberta</b> Sans frais : 310-0000 ATME sans frais : 1-800-232-7215 Site Web : <a href="http://www.servicealberta.ca">www.servicealberta.ca</a>
<b>Colombie-Britannique</b> Sans frais : 1-800-663-7867 ATME sans frais : 1-800-661-8773 Site Web : <a href="http://www.gov.bc.ca">www.gov.bc.ca</a>	<b>Yukon</b> Sans frais : 1-800-661-0408 ATME : (867) 393-7460 Site Web: <a href="http://www.gov.yk.ca">www.gov.yk.ca</a>	<b>Territoires-du-Nord-Ouest</b> Téléphone : (867) 873-7817 Site Web : <a href="http://www.gov.nt.ca">www.gov.nt.ca</a>
<b>Nunavut</b> Téléphone : (867) 975-6000 Site Web : <a href="http://www.gov.nu.ca">www.gov.nu.ca</a>		

Pour obtenir de l'information au sujet de la fraude par carte de débit et des dossiers de crédit, veuillez communiquer avec l'Agence de la consommation en matière financière du Canada en composant le 1-866-461-ACFC (2232) (for services in English: 1-866-461-FCAC (3222) ou visiter son site Web à [www.fcac-acfc.gc.ca](http://www.fcac-acfc.gc.ca).

# La Déclaration de vol d'identité : Questions souvent posées

---

## Qu'est-ce que la déclaration de vol d'identité?

- La déclaration de vol d'identité est un formulaire créé par le gouvernement, qui vous aide à produire de la documentation écrite au sujet d'un vol d'identité.
- La déclaration de vol d'identité est un formulaire que vous pouvez utiliser pour aviser les institutions financières, les sociétés émettrices de carte de crédit et d'autres entreprises que vous avez été victime d'un vol d'identité, et leur fournir l'information dont elles ont besoin pour faire enquête au sujet de l'incident. Ce ne sont pas toutes les entreprises qui acceptent la déclaration; certaines exigent d'utiliser leur propre formulaire. Communiquez avec l'entreprise avant de lui transmettre la déclaration afin de connaître ses exigences.

## Pourquoi devrais-je utiliser la déclaration de vol d'identité?

- Dans le but d'enquêter sur un incident et de corriger leurs dossiers, les entreprises (institutions financières, sociétés émettrices de carte de crédit et autres entreprises) exigent de recevoir l'information de la victime. Vous pourriez être en mesure de fournir l'information nécessaire au téléphone, mais dans certains cas l'entreprise exige de la recevoir par écrit.
- Certaines entreprises accepteront la déclaration de vol d'identité afin d'obtenir l'information dont elles ont besoin pour amorcer une enquête. Au lieu de vous procurer les formulaires utilisés par chaque entreprise et de les remplir l'un après l'autre, vous pouvez remplir un seul formulaire et en envoyer une copie à chaque entreprise, si chacune accepte la déclaration. Vous gagnerez ainsi du temps et aiderez à simplifier le processus permettant de combattre la fraude et à blanchir votre réputation.
- Même si une entreprise n'accepte pas la déclaration de vol d'identité, le fait de rassembler tous les renseignements important au sujet de l'incident dans un seul document peut vous aider lorsque vous remplirez les formulaires des entreprises.

## Comment les entreprises utiliseront-elles la déclaration de vol d'identité?

- Les institutions financières, les sociétés émettrices de carte de crédit et d'autres entreprises qui acceptent la déclaration de vol d'identité se serviront des renseignements contenus dans la déclaration pour amorcer une enquête sur l'incident. Elles pourraient vous demander d'autres renseignements pour faciliter l'enquête.
- Le fait de remplir la déclaration de vol d'identité ou tout autre formulaire exigé par l'entreprise ne garantit pas que le voleur d'identité soit poursuivi en justice ou que vous soyez exonéré de la responsabilité ou de la dette.

## Comment dois-je remplir la déclaration de vol d'identité?

- Après avoir effectué tous les appels téléphoniques importants, remplissez la déclaration de vol d'identité (et tout autre document nécessaire) aussitôt que vous constatez que l'incident s'est produit. Ainsi, les enquêtes pourront être amorcées rapidement et les dommages pourront être limités.
- Fournissez autant de renseignements que possible. L'entreprise pourra ainsi mener son enquête et procéder à votre remboursement.

- Remplissez les deux parties de la déclaration :  
La Première partie est réservée aux renseignements à votre sujet et à ceux relatifs à l'incident. La Deuxième partie est consacrée aux renseignements spécifiques au sujet de vos comptes et des activités. **Remplissez cette partie séparément pour chaque entreprise que vous avisez, et envoyez à chaque entreprise que l'information relative aux comptes ou aux activités ayant trait à l'entreprise en question.**
- Lorsque vous aurez rempli et signé la déclaration, joignez-y une copie (non pas l'original) de tous les documents à l'appui dont vous disposez (par exemple, relevés d'opérations, reçus, rapport de police). Conservez dans vos dossiers une copie de tout ce que vous soumettez.

### Où dois-je envoyer la déclaration de vol d'identité?

- Fournissez une copie de la déclaration de vol d'identité remplie et des pièces jointes à chaque entreprise qui a fourni du crédit non autorisé, de l'argent, de l'information, des biens ou des services au voleur qui s'est emparé de votre identité, et qui accepte la déclaration. Faites-lui parvenir par courrier recommandé. Toutefois, n'envoyez pas la déclaration aux organismes gouvernementaux.

### Comment puis-je savoir que mes renseignements personnels sont protégés lorsque je soumetts la déclaration de vol d'identité?

- Les entreprises qui reçoivent la déclaration de vol d'identité doivent s'assurer que les renseignements personnels que vous avez fournis soient protégés et utilisés uniquement aux fins de l'enquête sur l'incident décrit dans la déclaration, pour poursuivre la ou les personnes responsables et pour prévenir d'autres fraudes ou vols. Les entreprises peuvent divulguer les renseignements aux institutions ou organismes responsables de l'application de la loi uniquement à de telles fins. Les renseignements ne peuvent être utilisés ou divulgués pour aucune autre fin, sauf celles autorisées par la loi.
- Vous pourriez vouloir prendre des précautions lorsque vous soumettez la déclaration de vol d'identité. À titre d'exemple, si l'entreprise a une succursale ou un bureau dans votre quartier, vous pourriez lui livrer en personne la déclaration de vol d'identité. Autrement, vous devriez l'envoyer par courrier recommandé.
- Vous devriez garder une copie de tous les documents que vous fournissez et la conserver en lieu sûr.

### J'ai adopté toutes les mesures suggérées. À quoi dois-je m'attendre maintenant?

- En adoptant rapidement les mesures décrites précédemment, vous pouvez aider à freiner l'imposteur et ainsi limiter les dommages, et amorcer le processus permettant de blanchir votre réputation. Malheureusement, ce processus peut exiger de vous du temps et des efforts : rédaction de lettres, appels téléphoniques, présentation de documents et autres renseignements. De plus, le problème pourrait ne pas être réglé immédiatement.

Les mesures suivantes peuvent aider à résoudre l'incident :

- Consignez tous vos appels téléphoniques - prenez en note le nom de toutes les personnes à qui vous vous êtes adressé, le contenu de votre entretien, et la date de votre conversation.
- Dans des situations complexes, vous pourriez vouloir assurer le suivi par écrit avec les personnes-ressources avec qui vous vous êtes entretenu au téléphone ou en personne.
- Conservez l'original des documents à l'appui, comme les rapports de police, les lettres adressées aux entreprises et celles qu'elles vous ont envoyées; n'envoyez que des copies.
- Conservez les vieux dossiers même si, à votre avis, le cas semble réglé. Des erreurs pourraient réapparaître dans vos dossiers de crédit ou vos renseignements personnels pourraient circuler de nouveau. Si tel était le cas, vous serez heureux de les avoir conservés.

# DÉCLARATION DE VOL D'IDENTITÉ

À : \_\_\_\_\_  
(nom de l'institution financière, la société prêteuse, ou autre entreprise)

## Première partie : Renseignements à votre sujet et sur l'incident

Je, \_\_\_\_\_, affirme ce qui suit :  
(nom)

### Renseignements personnels

(1) Mon nom légal complet :

\_\_\_\_\_  
(prénom) (deuxième prénom) (nom)

(2) Le prénom que j'utilise (si différent du prénom ci-dessus) :

\_\_\_\_\_  
(prénom) (deuxième prénom) (nom)

(3) Ma date de naissance (a/m/j) : \_\_\_\_/\_\_\_\_/\_\_\_\_

(4) Mon adresse : \_\_\_\_\_

Ville : \_\_\_\_\_ Province/Territoire : \_\_\_\_\_ Code postal : \_\_\_\_\_

(5) Mon numéro de téléphone à la maison : \_\_\_\_\_

(6) Mon numéro de téléphone au travail : \_\_\_\_\_

(7) Je préfère qu'on communique avec moi :

À la maison

Au travail

À un numéro différent : \_\_\_\_\_

**Renseignements sur l'incident**

**Veillez cocher toutes les affirmations pertinentes**

8)  J'ai eu connaissance de l'incident comme suit : \_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_

9)  Je n'ai autorisé personne à se servir de mon nom ou de mes renseignements personnels en vue d'obtenir l'argent, le crédit, les prêts, les biens ou les services décrits dans le présent document.

10)  Je n'ai retiré aucun profit, aucune somme, aucun bien ou service par suite des événements décrits dans le présent document.

11)  Mes pièces d'identité (p. ex. permis de conduire, passeport, carte de NAS, acte de naissance) :

\_\_\_\_\_ ont été perdues le ou vers le (a/m/j) \_\_\_\_\_/\_\_\_\_\_/\_\_\_\_\_  
\_\_\_\_\_ ont été volées le ou vers le (a/m/j) \_\_\_\_\_/\_\_\_\_\_/\_\_\_\_\_  
\_\_\_\_\_ n'ont jamais été reçues.

Autres renseignements (p. ex., noms des cartes, circonstances) :

\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_



Nom \_\_\_\_\_

## Documentation

*Veillez faire mention des documents justificatifs que vous êtes en mesure de fournir. Joignez au présent document des copies lisibles (conservez les originaux) de chacun de ces documents.*

14)  Une copie du rapport de police ou de l'organisme chargé de l'application de la loi (si disponible).

15)  Autres documents justificatifs : (Description) : \_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_

## Deuxième partie : Déclaration d'activités non-autorisées sur un compte

Remplissez cette section séparément pour chaque entreprise que vous avisez.

En conséquence des événements décrits dans la déclaration de vol d'identité (cochez tous les énoncés qui s'appliquent) :

- Le ou les comptes décrits dans le tableau ci-dessus (c.-à-d. compte chèques, compte d'épargne, carte de crédit, etc.) ont été ouverts par votre entreprise à mon nom, à mon insu, sans mon autorisation ou mon consentement, en utilisant mes renseignements personnels ou mes pièces d'identité.
  
- On a accédé à mon ou à mes comptes décrits dans le tableau ci-dessous (c.-à-d. compte chèques, compte d'épargne, carte de crédit, etc.), on les a utilisés ou débités à mon insu, sans mon autorisation ou mon consentement, en utilisant mes renseignements personnels ou mes pièces d'identité.

La fraude a été perpétrée par (si les circonstances sont connues) :

- une transaction en personne
  - un guichet automatique bancaire (GAB)
  - un achat à un point de vente
  - une transaction par Internet
  - une transaction par téléphone
  - un chèque
  - autre \_\_\_\_\_
  - je ne sais pas
- 
- Le ou les produits de crédit décrits dans le tableau ci-dessous (c.-à-d. prêt, hypothèque, ligne de crédit) ont été obtenus de votre entreprise en mon nom à mon insu, sans mon autorisation ou mon consentement, en utilisant mes renseignements personnels ou mes pièces d'identité.

Nom \_\_\_\_\_

### Description des activités non autorisées dans le ou les comptes

Nom et adresse de l'entreprise	Type de compte / N° de compte	Description de l'activité non autorisée (si connue)	Date (si connue)	Montant (si connu)
Exemple : Banque ABC 123, rue Principale, Ville	Compte chèques 1234567-890	Retrait	2001/01/02 ou : toutes les activités depuis le 2001/01/02	500 \$

Joindre des feuillets supplémentaires au besoin

Si l'incident porte sur une **hypothèque**, veuillez indiquer :

Nom et adresse de l'entreprise	Date d'enregistrement (si connu)	Description légale de la propriété	Adresse civique de la propriété	Numéro d'enregistrement de l'hypothèque (si connue)

Joindre des feuillets supplémentaires au besoin

- Au moment où la ou les incident(s) décrits ci-dessus se sont produits, je possédais le ou les comptes suivants auprès de votre entreprise (veuillez inscrire tout compte non mentionné ci-dessus) :

Nom pour la facturation

\_\_\_\_\_

Adresse de facturation

\_\_\_\_\_

Numéro du compte ou de la carte

\_\_\_\_\_

Joindre des pages supplémentaires au besoin.

Nom \_\_\_\_\_

## Protéger vos renseignements personnels

Vous reconnaissez que les entreprises auxquelles vous fournissez la déclaration de vol d'identité peuvent utiliser les renseignements personnels qu'elle renferme uniquement aux fins de faire enquête sur l'incident décrit dans la déclaration, d'entreprendre des poursuites judiciaires contre la ou les personnes responsables et d'empêcher une nouvelle fraude ou un nouveau vol. Ces entreprises peuvent, à ces fins, communiquer les renseignements fournis aux organisations et aux agences d'exécution de la loi (par exemple, services de police).

Les entreprises conviennent que ces renseignements ne peuvent être utilisés ni communiqués à quelque autre fin que ce soit, sauf pour ce qui est autorisé par la loi. Si ce document ou les renseignements qu'il renferme doit être produit dans le cadre de procédures d'application de la loi (c.-à-d. devant un tribunal), l'entreprise pourra devoir fournir ou communiquer le document et les renseignements.

## Signature

**Toutes les déclarations contenues dans ce formulaire sont véridiques et complètes en tout point, au mieux de mes connaissances et croyances.**

\_\_\_\_\_  
Signature

\_\_\_\_\_  
Signature du témoin (personne non apparentée)

\_\_\_\_\_  
Nom (en lettres moulées)

\_\_\_\_\_  
Nom (en lettres moulées)

\_\_\_\_\_  
Date

\_\_\_\_\_  
Date

\_\_\_\_\_  
Numéro de téléphone

**La personne qui donne sciemment de faux renseignements dans la déclaration s'expose à des poursuites judiciaires.**