idassist®

Victim Toolkit

How to guard against identity fraud – and what to do if it happens to you.

A real threat to Canadians

If you're like most Canadians, identity fraud is something you've been aware of — and concerned about — for quite a while now. But a lot of Canadians think that it's not likely to happen to them, even though the facts show that it's already impacted 1 in 3 of us.[1]

Victims often have to spend 100+ hours restoring their identity. Worse, they suffer from stress and anxiety (74%), require time off work (22%), and fear for the financial wellbeing of their family, too (69%)[2].

This guide is designed to help you take critical steps toward preventing identity fraud. And if you think your personal information has been stolen or used fraudulently, it also contains all the information you should need to limit the fallout and start rebuilding your identity.

What you'll find inside:

The Basics: Key Terms and Concepts

Let's start with the basics — key terms and concepts that will help clarify what identity criminals are looking for and how they use the personal information they discover.

The terms identity theft and identity fraud are often used interchangeably, but they have slightly different meanings. Theft comes first — it's what enables fraud.

What is Identity Theft?

Identity theft is a serious crime that happens when someone steals your personal information with the intent to commit crime or fraud. Often, criminals wait weeks, months or years before actually putting stolen data to use. That's one reason identity theft tends to go undetected until it's too late.

What is Identity Fraud?

Identity fraud is the actual deceptive use of your personal information, without your consent, to commit crime or fraud. In many cases, the person who steals your personal information sells it on the black market (or the dark web) to the highest bidder. The more information they have to offer, the higher the price.

What information are criminals looking for?

Criminals are looking for Personally Identifiable Information, or PII. It's unique to you and it pinpoints who you are. That's why it's the information you need to safeguard and monitor.

PII includes your:

- **Full Name**
- **Home address**
- **Date of birth**
- **Birthplace**
- **Emails, usernames, and passwords**
- **Social Insurance Number**
- **Medical records**
- **Passport number**
- **Driver's license number**
- **Bank account information**
- **Personal Identification Numbers (PINs)**
- **Credit card information**
- **Mother's maiden name**
- **Signature**
- **Insurance information**
- **Military credentials**

How do criminals get your information?

Criminals can use a variety of techniques to get access to your personal information, including:

Skimming: Tampering with ATMs or point-of-sale terminals to steal credit card information without anyone noticing.

Phishing: Some email scams are well-designed to look like they come from valid sources (like your bank, or a work colleague).

Dumpster diving: Your mail often includes PII, and most of it ends up in the trash. The bad guys are willing to dig through garbage to find it.

Shoulder surfing: It only takes a second for someone to snap a picture of your ID in a public place.

Social media: Even a simple post about your vacation lets criminals know you're away — which makes it the perfect time to break in and steal your PII.

Phone scams: Impersonating the CRA, a bank representative or other authority is one way criminals trick unsuspecting Canadians into handing over PII.

How do criminals use your information?

Criminals can use your stolen or reproduced personal or financial information to:

- Access your bank accounts or open new bank accounts
- Write bad cheques
- Transfer bank balances
- Obtain a mobile phone
- Apply for loans, credit cards and other goods and services
- Make purchases
- Open new utility accounts
- File a tax return and claim a refund in your name
- Commit crimes and use your information in the event of an arrest or court action
- Seize ownership of your home through title fraud
- Obtain passports or receive government benefits
- Facilitate organized criminal and terrorist activities
- And much, much more

How to find out if your identity was stolen

Rather than waiting for something bad to happen, get proactive, and monitor your accounts for suspicious activity:

Review your bank and credit card statements in detail each month — look for anything unusual.

Check your credit scores and reports frequently. Note that Canada has two credit bureaus, and to see a full picture of your credit profile, you'll need information from each one.

Sign up for a trusted identity monitoring service, like ID Assist.

Bonus Tip!

Wondering if your email may already be exposed to criminals online? Try ID Assist's email checking tool to find out.

Preventing Identity Theft: 15 Practical Tips You Can Use Right Away

In order to commit crimes using your information, thieves need to obtain it first. The smartest thing you can do is to make it hard or impossible for them to get their hands on your PII.

Here's how.

1. Check your credit reports, bank and credit card statements regularly. Report anything unusual or suspicious to the relevant financial institution and to the credit bureaus — right away.
2. Keep the operating system on your computer and mobile devices up to date. Install security software. Create strong passwords and change them regularly.
3. Scan the news from time to time to stay up to speed on new scams
4. File your tax return early so criminals can't obtain your refund before you do.
5. If you need to enter PII on a website you trust, be sure the address starts with "https" (which means it's a secure site).
6. Don't share more than you need to on social media, and only connect with people you know. (See more tips for staying safe on social media in the next section of this toolkit)
7. Check your surroundings and shield your hand whenever you need to enter your debit or credit card PIN. Watch for shoulder surfers and check that ATMs haven't been tampered with.
8. Never provide financial account numbers or other information when you're talking on the phone in public. Someone may be listening.

9. Remove mail from your mailbox right away — before thieves can beat you to it. If you'll be away, request a mail hold. Consider installing a mailbox lock (and help the seniors in your life do the same).

10. Be skeptical. Unsolicited emails, telephone calls or mail may be an attempt to extract your personal or financial information.

11. Pare down the ID you carry in your wallet or purse (your social insurance card is a good example). Remove any cards you don't need and keep them in a secure place instead.

12. During transactions, swipe your cards yourself instead of allowing a cashier to do it for you. If you need to hand over your card, don't lose sight of it.

13. Memorize all PINs and passwords (or use a password manager tool).

14. Shred personal and financial documents before putting them in the garbage.

15. When you change your address, make sure you notify the post office and all the relevant financial institutions (your bank and credit card companies).

Bonus Tip!

Register for a trusted online identity and credit monitoring service.

ID Assist scours the internet (including the dark web) for signs that fraudsters have compromised your identity. You're alerted immediately so you can take action and limit the fallout. And expert investigators are on hand to guide you through the process.

Safe sharing: How to protect yourself on social media sites

When it comes to social media, it's not just your friends and family who are interested in all the details. Criminals can use basic information you post online to steal your identity.

Here's what you can do:

- Only connect with people you know in the real world.
- Don't post key details. These include your full name and address, date of birth, telephone number, Social Insurance Number, information about your finances or employment. Also take care not to post things like your mother's maiden name, or anything else that may allow thieves to answer security questions on banking sites.
- Take time to review the privacy and security settings on the sites you use, and adjust them to maximize your protection (while still being able to use the features you need).
- Don't allow social networking sites to scan or upload your email address book.
- Be skeptical about any messages you receive. Hackers steal accounts and send messages that look like they're from your friends.
- Be careful about installing third-party tools, apps and games on social sites. Criminals may use these add-ons to steal your personal information.

How to Report Identity Theft

If you think your information has been compromised, here's what to do and who you'll need to contact:

Step 01

Contact your local police force and file a report.

Step 02

Contact your bank/financial institution and credit card company.

Step 03

Contact the two national credit bureaus, Equifax and TransUnion, and place a fraud alert on your credit reports.

Step 04

Contact the Canadian Anti-Fraud Centre and/or other relevant organizations (depending on the type of breach).

Type of fraud or scam	Who to contact
Identity theft or internet fraud	■ The Canadian Anti-Fraud Centre (CAFC) ■ Your local police force ■ Your financial institution ■ Both national credit bureaus: Equifax Canada TransUnion Canada
Investment fraud	■ Your provincial or territorial securities regulator. (A list of all regulators is on the Canadian Securities Administrators website).
Tax fraud or a questionable charitable organization	■ Canada Revenue Agency
Consumer fraud or fraudulent business activity	■ Better Business Bureau ■ Your local police force
Credit card and debit card fraud	■ Your financial institution
General frauds	■ Canadian Anti-Fraud Centre ■ Local police

Bonus Tip!

ID Assist can fully handle identity restoration on your behalf, or guide you through the process.

How ID Assist Can Help

ID Assist is an early warning system that helps you look after your identity.

1. Input the personal information you want monitored: credit card number, passport number, driver's license, bank accounts and more. ID Assist's advanced technology combs the internet — including the dark web, where criminals buy and sell stolen ID — for signs of suspicious activity. It can even pull data from both Canadian credit bureaus.

2. You're alerted to trouble as soon as our systems spot it. Choose to be notified by email, text or through our mobile app. Then, you can take action to limit the damage.

3. If you are a victim, we have a team of Identity Theft Experts who will help you restore your identity, or do it for you if you prefer.

How the ID Assist team helps when you've been breached:

1. We'll contact Equifax & TransUnion on your behalf to place a fraud alert on your credit report.
2. If your credit and/or debit cards have been added for monitoring in ID Assist, we can contact your financial institution on your behalf to report the incident.
3. Our experts can guide you through the process required to restore your identity, from start to finish.

idassist®

Victim Toolkit

Get started with ID Assist

500,000+

Join the 500,000+ Canadians who trust ID Assist technology to help safeguard their identity.

To learn more about identity crime, visit these reliable sources.

- https://www.canada.ca/en/financial-consumer-agency/services/financial-toolkit/fraud/fraud-2/8.html
- http://www.rcmp-grc.gc.ca/scams-fraudes/id-theft voleng.htm
- https://www.canada.ca/en/financial-consumer-agency/services/financial-toolkit/fraud/fraud-2/5.html
- https://www.cooperators.ca/en/Resources/stay-safe/identity-theft-protection.aspx
- https://cba.ca/identity-theft
- http://www.ic.gc.ca/eic/site/oca-bc.nsf/eng/ca03025.html

1 https://www.cpacanada.ca/en/connecting-and-news/news/media-centre/2017/march/ cpa-canada-fraud-survey
2 https://www.idthefcenter.org/images/page-docs/AfermathFinal_2016.pdf