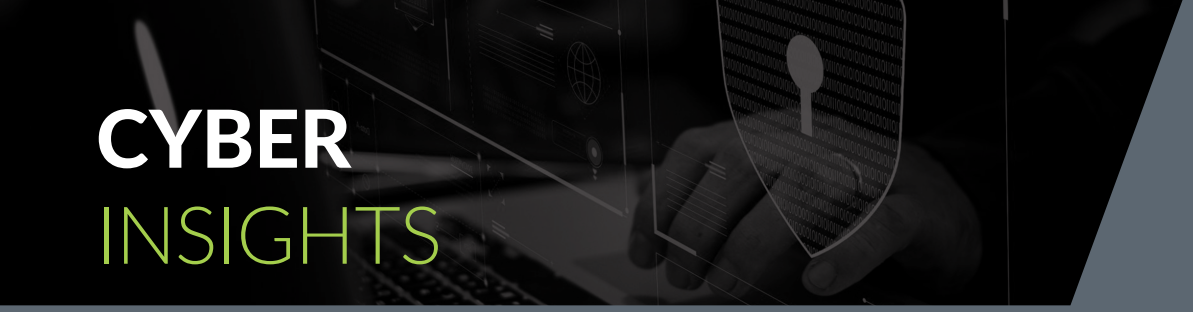

CYBER
INSIGHTS

LloydSadd

NAVACORD®

What To Do After a Data Breach

Getting notified that your data has been exposed in a cyberattack is harrowing. It's natural to feel something akin to a home break-in, even though nothing was stolen from your physical space.

Unfortunately, your data is in criminal hands once it's stolen. It could end up being sold on the dark web as part of a data bundle. Criminals buy data bundles to create phishing scams and false identities, or commit credit card fraud. Criminals could use your data immediately, or it could be part of a future scam.

Either way, your data is out there. The best thing you can do is step up your vigilance.

Fight the urge to give up or blame yourself after a breach. It's not your fault. Here are low- to no-cost actions you can take to help yourself.

COMPANIES MUST TELL YOU IF YOUR DATA WAS PART OF A BREACH

Under PIPEDA and provincial data privacy laws, companies are required to inform customers if their personal data is exposed in a breach and are encouraged to provide free credit monitoring for at least a year.

Companies that do background checks can become targets. Employers, landlords, financial institutions and individuals can purchase background checks to verify an applicant's information. In 2024, two major U.S. background check companies had data stolen, exposing over 10 million personal records. The exposed data records included names, emails, addresses, phone numbers, employment histories, birth dates and legal records. Time will reveal the extent of the data breach.

If your personal data was exposed as part of a cyberattack on a company, they should notify you.

WHAT A DATA BREACH COMMUNICATION MIGHT LOOK LIKE

A company may offer you a single credit monitoring service or a suite of services, which can include:

- **Credit monitoring.** This service monitors your credit reports from the two major credit reporting agencies: Equifax and TransUnion.
- **Identity monitoring services.** These monitor internet and database sources, including criminal records, arrest records, bookings, court records, payday loans, bank accounts, checks, sex offenders, change of address requests and Social Insurance number traces.
- **Identity restoration services.** An agency works with you to restore your identity.
- **Identity theft insurance.** This covers identity theft that occurs during the coverage period. It may cover expenses incurred to restore your identity. Check your policy for coverage dates, exclusions and deductibles for specific events.

The type of services you're offered may depend on your location and the severity of the exposure.

For example, you may only be offered credit monitoring if you were potentially affected but not confirmed as part of the breach. If your data was confirmed as exposed due to the breach, the company might offer you a comprehensive suite of services.

IF YOU'RE NOTIFIED OF A DATA BREACH

Use the credit monitoring services companies offer you. If you have identity theft protection, tell your service about the breach notification.

It's good data hygiene to monitor your credit profile,

regardless of a data exposure event. But it's critical if you're involved in a data breach. Monitor your credit card and health care statements, as well as your credit reports and tax return activity.

Watch for charges you did not make on your credit cards or services you did not receive on your explanation of benefits statements. If you see suspicious activity, contact the relevant institution immediately.

REPORTING IDENTITY THEFT

Once your data is being used for unauthorized activities, you're in the stages of full-blown identity theft. If you believe you are the victim of identity theft, report it. By the time you reach this stage, the damage has often been done. It can be overwhelming to handle alone, so it's best to take minute and breathe:

- Report the fraud to the Canadian Anti-Fraud Centre, a taskforce managed by the RCMP, OPP and the Competition Bureau Canada.
- Contact your local law enforcement authorities to file a complaint. Even if they don't investigate it, you can reference the police report number when filing credit card and other disputes.
- Activate an alert on your credit report to prevent criminals from opening credit accounts in your name. The two main credit reporting bureaus in Canada are:

Equifax: 800-465-7166

TransUnion: 800-663-9980

FRAUD ALERTS AND SECURITY FREEZES

A fraud alert or security freeze (or both) can help protect you from identity theft. Both are free, and you can activate them using the major credit reporting bureaus listed above. Learn the key differences below.

FRAUD ALERTS

Placing a fraud alert on your credit reports tells potential creditors to verify your identity before opening new credit accounts in your name. Creditors should contact you directly or take other steps to verify your identity.

When a creditor runs your report, they'll see the fraud alert. This tells them to take extra precautions to verify it's you. Usually, they'll contact you at the number you provided when you requested the fraud alert. Keep track of the contact information you provided on the fraud alert and update it if you change your information.

SECURITY FREEZES

While a fraud alert adds an extra verification step, a "security freeze" or "credit freeze" locks down your credit file entirely. While your current accounts remain active, no new accounts can be opened in your name.

A security freeze remains in effect until you choose to lift it. Although it offers more secure protection, a credit freeze makes applying for credit, buying a house or renting an apartment inconvenient. You need to remember to lift the freeze first or the creditor will deny your application.

WHAT TO DO IF YOUR IDENTITY HAS BEEN STOLEN

Maybe you notice an unfamiliar charge on your credit card statement or you get a call about an overdue account that you never opened. Chances are good your identity has been stolen and the fraudster has opened several accounts in your name. Even if the fraud involves only one account, you'll still need to check all of your accounts.

REPORTING ON YOUR OWN

The Canada Revenue Agency (CRA) recommends you report your identity theft to the following:

- Your financial institution
- Local law enforcement;
- The CRA at 1-800-959-8281;
- A credit reporting agency such as Equifax or TransUnion;
- 1-800-O-Canada (1-800-622-6232) for information on where and how to replace identity cards such as your health card, driver's licence, or SIN if necessary
- The RCMP's Phonebusters by email at info@phonebusters.com or call 1-888-495-8501 if your identity theft occurred as part of a scam

IDENTITY THEFT INSURANCE

If you have identity theft insurance as a stand-alone policy, as an add-on through your home or renters policy, or as part of a data breach exposure settlement, alert your insurance company. Identity theft insurance won't reimburse you for money stolen, but it will help you with steps toward credit recovery. They'll handle everything.

MINOR CHILDREN AND CREDIT REPORTS

Your children don't typically have a credit report unless you add them as authorized users on your credit card accounts or hold a joint account with them. Criminals can commit fraud using a child's personal information and go undetected for years. You can request a credit report from TransUnion or Equifax. If you enroll in an identity protection service, they often offer family plans.

CREDIT MONITORING AND FINANCIAL INFORMATION RESOURCES

Make it a habit to monitor your personal information, whether you're involved in a breach or not.

- You can access your credit report only for free with Equifax and TransUnion. You can also order your report by mail or phone.
- Use secure passwords, update your software and sign up for multifactor authentication.
- Stay proactive after a data breach. Companies and the government provide mechanisms to safeguard victims from further exploitation.

Call your insurance broker if you're interested in identity theft protection. You might be able to add it to your home insurance policy for a small premium increase. Remember, you won't be covered for a breach you're already aware of. Call before an incident to save yourself a major headache.

If you have questions specific to your business, or would like additional information, please reach out to your Lloyd Sadd Advisor.

LET US HELP YOU MANAGE YOUR RISK

Edmonton: 1.800.665.5243
Calgary: 1.866.845.8330
Kelowna: 1.800.665.5243

lloydsadd.com
info@lloydsadd.com