What to Do if Your Information Has Been Stolen

Identity theft can happen to anyone. Since more people are going online to shop, bank, file taxes, etc., there's an increased risk of savvy thieves stealing the personal information of millions of consumers. Even if you're careful, a thief may be able to attain your information by hacking into the systems of larger businesses, as millions of people learned last year with the Equifax data breach, which impacted more than just Americans; it impacted 100,000 Canadians as well.[1] In this breach, hackers stole personal information and credit card numbers through a consumer website application that was intended for US consumers. Equifax Canada's systems were not impacted. Stolen information allows thieves to open bank accounts and lines of credit, open new credit cards and more. What can you do if you find out your information has been compromised?

The rise of data breaches

Equifax isn't the only company to endure a data breach in the last few years. Other notable data breaches include CVS and Walmart Canada; in both cases, credit card information was compromised by way of the companies' online photo processing websites. According to a recent study, more than 59 data breach incidents occurred in the first six months of 2017, exposing the personal information from approximately 2.1 million records.[2] As a result, the Canadian government is considering new regulations that would require companies to report data breaches; at the provincial level, only Alberta currently requires companies to do so.[2]

Additionally, even email providers aren't safe from data breaches. It's recently come to light that Yahoo's 2013 breach, in which names, email addresses, telephone numbers, dates of birth, passwords and security questions were stolen, impacted all of its three billion users, including many Canadians. People were encouraged to change their passwords, as well as their security questions and answers.

What to do if you're the victim of a data breach:

As we've seen, you may not know you're the victim of a breach until you hear about it on the news. The first thing you should do if you suspect you're a victim is to **check your credit reports** from both Equifax Canada and TransUnion Canada. The report is free if you request by mail. The process may vary by credit bureau so refer to their websites for instructions.

Next, **monitor your credit card and bank accounts for unauthorized activity** and review each charge carefully. Equifax Canada allows Canadian adults to **place an alert** on their credit files. The company also offers three types of file alerts: 1. Identity alerts for residents of Manitoba and Ontario; 2. Lost or stolen alerts if a person has misplaced their personal identification or financial information or had it stolen; and 3. Fraud alerts in response to suspicious credit applications or unauthorized charges. These alerts warn creditors that your information was stolen and prompts them to verify the identity of anyone looking to get credit in your name. In Manitoba and Ontario, credit bureaus are required to offer credit alert services to residents. However, even with these tools available, it is still up to you to monitor your credit and report any unauthorized or suspicious activity.

Scott Arial

ROYAL LEPAGE
Team Realty
Independently Owned and Operated, Brokerage

Royal LePage Team Realty
Real Estate Broker
484 Hazeldean Road
Kanata, ON K2L 1V4
613.592.6400
613.850.4542

scottarial@royallepage.ca
www.scottarial.com

What to do if your information has been stolen:

Although credit card microchips have curtailed counterfeiting thieves have become focused on opening new accounts with stolen information. From January 2014 to December 2016, Canadians lost an estimated $290 million to fraud and scams.[3] Older Canadians tend to be the largest target for thieves; Canadians between the ages of 60 and 79 lost $28 million in scams during the same period of time.[3] If you learn your information has been compromised, here are some steps to take to regain control of your information. In every situation, you'll want to contact your local authorities to report the theft, as your bank and creditors may require a report number to recover your money. Also, continue to check your credit report and report any additional unauthorized activity.

If your debit or credit card number has been stolen:

- Contact your bank or credit card company to cancel your card and get a new one.
- Review all of your transactions and call the fraud department if you notice fraudulent charges.
- Update your automatic payments with the new card number as soon as it arrives.

If your bank account information has been stolen:

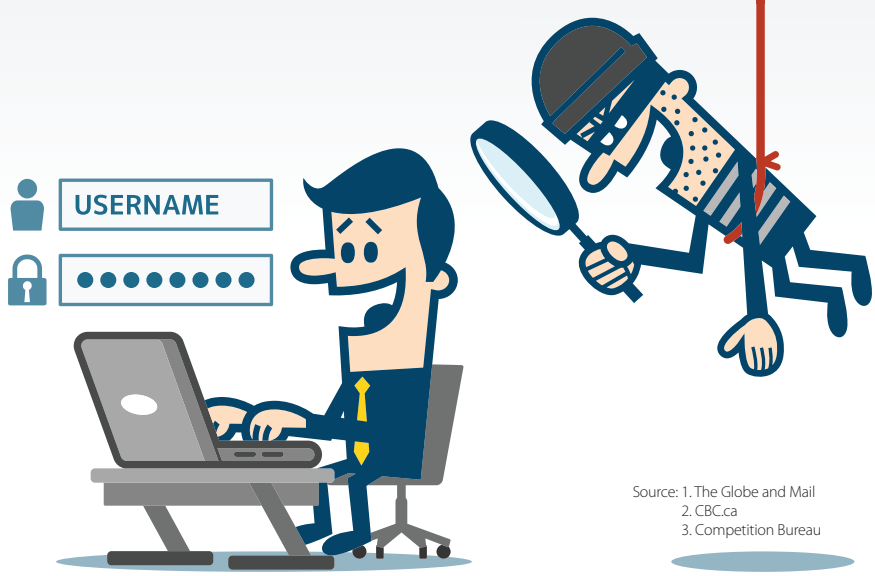
- Contact your bank to close your account and open a new one.
- Review your transactions and contact the fraud department to report false charges.
- Update automatic payments with your new information.

If your driver's licence information has been stolen:

- Contact a registry agent for a new licence.
  You'll need to provide valid identification and pay a fee.

Identity fraud: An underreported crime

Only an estimated five percent of fraud is reported to the authorities.[3] Why don't more people report their information stolen? According to a recent study, they may feel too embarrassed. Others didn't report because the amount stolen was so small, they didn't want to go through the hassle. In other cases, there's a perception that it's not a *"real"* crime. The same research suggests that businesses don't report data breaches because they don't want to look vulnerable and damage their brands.[3]



Source: 1. The Globe and Mail
2. CBC.ca
3. Competition Bureau

What if a child's information has been stolen?

Thieves may be able to get a hold of your child's personal information. Unfortunately, you may not become aware of a compromise until they try to find employment, rent an apartment or get a loan for school or a car.

- **Check with each credit bureau to see if they have a credit report.** If your child is about to turn 16, you may want to do this, even if you don't suspect their identity has been stolen. If they have a credit report, request a copy and use the information they provide to remove all fraudulent activity. You may also ask each of the credit reporting companies to do a manual search of the child's file.
- **Send letters requesting the companies remove all accounts, inquiries and collection notices** in your child's name or information.
- **Contact the businesses** where the child's information was used.
- **Limit who has access to your child's personal information.** Read the notices sent from your child's school pertaining to directories and how your child's information is used.