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. Cyber breaches increased to 1,093 in 2016, up from 780 in 2015, with most of these breaches impacting medical/health care organizations, education and government/military sectors.[1] As of October 2017, there were 1,056 breaches reported, which exposed more than 171 million records.[1] According to experts, stolen information can sell for more than $30 per identity on the black market.[2] However, in time and frustration alone, it'll cost a victim much more than that. Stolen information allows thieves to open bank accounts and lines of credit, open new credit cards, get a driver's license in your name, file taxes to steal your tax refund and more.[2] What can you do if you find out your information has been compromised?

The rise of data breaches

The Equifax data breach in 2017 showed that even if you're vigilant about protecting your personal information, it may still be compromised. In this breach, hackers stole information from 143 million Americans, including people's names, Social Security numbers, birth dates, addresses and driver's license numbers, as well as the credit card numbers of 209,000 people.[3] Thieves were also able to gain access to information from 182,000 individuals who filed credit disputes with Equifax prior to the breach.[3]

Equifax has set up a page for those who may have been impacted: **Equifaxsecurity2017.com**. Due to the size of the breach, Equifax has made everyone eligible for a year of free credit monitoring.

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. 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 all of your credit reports—Equifax, Experian and TransUnion—by getting a free credit report at **annualcreditreport.com**. If you've already accessed your credit report this year, you may have to pay a fee.

Next, **monitor your credit card and bank accounts for unauthorized activity** and review each charge carefully. If you find or suspect you're a victim of fraudulent activity, **put a freeze on your credit file.** This makes it more difficult for a thief to use your info to open a new account in your name; however, it won't prevent them from making charges to your current credit accounts. The freeze lasts until you remove it; however, in Kentucky, Pennsylvania and South Dakota, the freeze lasts seven years.[4]

You may also **place a fraud alert on your credit file** to warn creditors that your identity was stolen. This will prompt them to verify the identity of anyone looking to get credit in your name.

Additionally, **file your taxes early** to prevent a scammer from filing for you and collecting your refund.

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.[1] More than $16 billion was stolen from 15.4 million American consumers in 2016.[1] Identity thieves have stolen more than $107 billion since 2010.[1] 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 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 license information has been stolen:

- Contact the DMV and report your license stolen. The state may then flag the number in case someone tries to use it.

How thieves have used stolen information[1]

34% employment or tax-related fraud

29.2% tax fraud

32.7% credit card fraud

25.6% new accounts

16% other identity theft

13.1% phone or utilities fraud

11.8% bank fraud, involving checking, savings, other deposit accounts, debit cards and electronic fund transfers

6.8% loan or lease fraud

6.6% government documents or benefits fraud

Sources: 1. Insurance Information Institute
2. CNN
3. FTC
4. Kiplinger's Personal Finance

What if your 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.
- **Request a credit freeze for your child**, if your state allows it. Go to the websites of each credit bureau for instructions.
- **Send letters requesting the companies remove all accounts, inquiries and collection notices** in your child's name or information. Be sure to include a copy of the Uniform Minor's Status Declaration available on the Federal Trade Commission's website.
- **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. You have the right, under the federal Family Educational Rights and Privacy Act (FERPA), to opt out of sharing your child's contact and other directory information with third parties.