If Your Identity Has Been Stolen, Here's Exactly What to Do Next

thepennyhoarder.com/save-money/identity-theft-what-to-do

February 23, 2021

see more from Save Money

by Tiffani Sherman

Contributor

Reviewed by Molly Moorhead, CFP®

It all started with an alert.

In February 2019, I was on vacation in a foreign country when I received an email confirming I had just used all of my airline points to buy gift cards. Then came another telling me I had done the same with all of my hotel points.

The problem is, I had done neither of these things.

I panicked.

I frantically tried to contact both companies to report the fraud. Both tried to send me password change requests, which I wasn't receiving. They locked down my accounts.

Then I started getting other notices and alerts. Someone had my logins for several sites, and nefarious things were occurring very quickly.

Fast forward to December of 2020 when I got another alert. Someone had tried to apply for several credit cards, loans and unemployment assistance in my name and using my information.

I panicked… again.

Then the snail mail letters started arriving saying different financial institutions and government agencies needed more information in order to approve my loans and requests for assistance.

Again someone was using my personal information to commit fraud and steal my identity.

According to the 2020 Identity Fraud Report released in May 2020 by Javelin Strategy & Research, there were 13 million cases of identity fraud in 2019 costing $16.9 billion.

Identity theft has certainly taken a lot of my time to fix problems and restore my accounts to their pre-theft condition.

I have learned a lot along the way about what to do when you become a victim of identity theft.

How We Got Here

The Javelin report predicts criminals will continue to try to take what is not theirs by doing what they did to me. We are making it too easy for them.

“We’ve been tethered to sort of pre-technological advances,” says John Buzzard, Fraud & Security Analyst for Javelin Strategy & Research. “We’ve been tethered by certain identifiers that are incredibly dangerous because they’re stale and they’re everywhere.”

He’s referring to things like Social Security numbers, date of birth and knowledge-based questions.

“All of that stuff worked for a very long time because we really didn’t have the socio-technological advancements,” Buzzard said.

Now we’re a convenience society used to paying at the gas pump, swiping credit cards and shopping online. And even though we probably don’t think so, we’ve overshared information, he warned.

Combine that with what is available from public records and a pretty complete picture of a person is easily available online.

Google yourself. It’s terrifying.

The Javelin survey says the technology is there to better protect us, but consumers are not always quick to adopt it. It also suggests the conversation needs to shift from monitoring activity to better securing information so it can’t be stolen in the first place.

But until that happens, information is going to get into the wrong hands. If yours does, there are several things you should do to control the damage.

Protect What is Yours

When you watch someone drain your accounts in real time like I have, protecting what you have from further damage is imperative and time-sensitive.

The first thing to do is grab a notebook and write down everything you do to stop the bleeding. While frazzled, it's difficult to remember what you have and haven't done as far as changing passwords, notifying companies, etc.

Some of the reports you will need to fill out will require details and those details can be difficult to remember.

Take note of:

- Which accounts are impacted, how they are impacted and when it happened..
- The name and company ID number of any person you talk with about the theft and when you talk with them.
- That person's phone number.
- What they tell you to do so you can check things off as you do them.

Screenshots and photos are also helpful, especially to track account balances.

Change Passwords

Once you become aware of any problem, change passwords immediately on every email, bank, credit card and e-commerce account.

This is very important because many companies send a message to reset a password and if a scammer has control of your email account, you won't get them. They will.

That was part of my problem during my first round of ID theft. I didn't realize it, but someone had my email password and had set up forwarding of all of my emails containing certain keywords. So I didn't see that they were ordering things and resetting passwords.

Increase Account Security

Enable two-factor authentication for everything you log into. What this does is require a code in addition to a password to log in. The one-time code is often sent via email, text message or phone call.

Contact any financial institution you currently do business with. They can flag your accounts and add additional security measures beyond what is usually available.

"You have to protect the relationships that you have that are real, and most of those companies out there today — whether it's your bank or credit card or utility — identify and authenticate you and add a variety of security phrases to your account. So that if somebody calls in and tries to do a verbal account takeover, they will need a security phrase," Buzzard said.

Remember, you will also need that security phrase when you call in for any reason to authenticate your identity.

After Tiffani Sherman's identity was stolen, she filed reports with law enforcement and reported the fraud to every financial institution where someone tried to use her information. Pictured is a letter from one of the financial institutions confirming Sherman's case. Chris Zuppa/The Penny Hoarder

Keep Information Current

Make sure businesses you do business with have up-to-date information about how to find you. They can't tell you about fraud if they can't reach you.

"There's a great deal of people that don't change their addresses with (their bank or other account holders) because they file a forwarding order and then they're lazy for an entire year because they know that their mail is going to follow them," Buzzard said.

Other measures you might want to take:

- **File a Form 14039 with the IRS**: This IRS identity theft affidavit will notify the Internal Revenue Service that someone has your personal information and might try to file a tax return using your Social Security number and get your refund if you are eligible for one.
- **Get an IP PIN for the IRS:** The Identity Protection PIN is a six-digit number that will keep someone from filing a tax return electronically using your Social Security number. Each tax year, you will receive a new IP PIN to use to file.
- **Check your Social Security Statement:** Using an account with the Social Security Administration, you can check your earnings on your Social Security Statement to make sure they are correct.
- **Check with the DMV:** If you think someone has used your driver's license number to commit fraud (like using your DL number and personal information with their photo), it's possible to monitor that number and sometimes even change it.
- **Track your logins:** Many platforms will tell you when you last logged in. This can help if it shows a login at 3 a.m. and you were in bed at 3 a.m.

Protecting Your Credit

It's very important to protect your credit.

Placing a fraud alert on your credit is a method of security. Contacting one of the three credit bureaus, Equifax, Experian, or Transunion will place a one-year fraud alert for all three.

But fraud alerts are far from fool-proof.

“A fraud alert is a notice on your credit report that says anyone has to contact you and check with you before granting credit. That should be a good protection and if it worked like [the bureaus] said, it would be,” said Steven Weisman, an expert in identity theft and cybersecurity and founder of Scamicide. “But quite frankly, most of the time fraud alerts are ignored and there’s no significant penalty if a company doesn’t call you and honor a fraud alert.”

A basic fraud alert expires after one year. After that there will be no protection on your credit.

A better way to protect your credit is by placing a credit freeze with each of the three credit bureaus. Doing this is supposed to stop any application for credit in your name from being approved.

“It’s not too late for someone who already has their information out there,” Weisman said. “As a matter of fact, it’s even more important because you know they have your information.”

Here are links to the three major credit bureaus to freeze your credit.

- Equifax
- Experian
- Transunion

While you’re logged into their websites, request a copy of your credit report from each one and study it. Your credit report contains a list of any open lines of credit you have and anything you have applied for during a certain period of time.

Looking at my credit report, I noticed several more attempts to apply for credit I was not aware of. Each bureau’s report contains different information so it’s important to scour each one.

If you find something that isn’t accurate, write down the financial institution, the date of the credit inquiry and any other information listed. You’ll need it later.

Finally, open a dispute about anything that is not accurate. Keep track of any disputes you file and make sure they are removed.

After finding out her identity was stolen, Sherman called the non-emergency number of her local Sheriff’s Office. They took her information and someone from the Investigative Operations Bureau in the Economic Crimes Unit called to follow up. Chris Zuppa/The Penny Hoarder

File Reports with the Right Authorities

Two questions everyone will ask you when you talk about identity theft: Do you know who stole your information, and do you think law enforcement will catch them?

While I'd like to think the people who caused me so much trouble will end up in handcuffs, realistically I know that probably won't happen.

Even so, you should file a report with your local law enforcement and the Federal Trade Commission. Many financial institutions will ask for copies of these reports when you report fraud to them.

For the reports, you will need all the information you wrote down about each incident to document what happened to you.

I called the non-emergency number to my local Sheriff's Office and after they took my initial information, someone from the Investigative Operations Bureau in the Economic Crimes Unit called me and asked for details about each incident.

After a couple of weeks, I was able to request a copy of that report.

The report with the FTC allows you to tell them what happened and get a personal recovery plan. You can also download and save a copy of this report.

Report the Fraud to the Financial Institutions Involved

Congratulations. You just finished the easy steps in dealing with identity theft. It gets harder and much more frustrating from here.

Now you need to start contacting each financial institution where someone tried to use your information and report it as fraud.

With my recent go-around, I began receiving letters either asking for more information to complete applications, telling me about denials or welcoming me to their financial "family."

Each letter means at least one phone call — and often many more. Sadly, the onus is on the victim to prove something is theft.

Every time I called the phone numbers on the letter and told them I wanted to report fraudulent activity, they said they needed information to verify my identity.

Guess what they asked me? The same information the scammers had used to apply for the accounts in the first place, usually name, address, Social Security number and date of birth.

Rarely was everything finished after one phone call. Several institutions required me to send them copies of either the FTC or law enforcement report, or both. Others are making me fill out their forms.

My frustration level rises with each phone call.

Eventually, you will receive letters from each financial institution saying they have completed their investigations, reported the activity as fraud and asked for it to be removed from your credit reports.

Stay Vigilant

Sadly, now that my information is out there, I know there is a chance I will be a victim of identity theft again.

“It doesn’t mean that you’re going to constantly be hacked, but it does mean that you’re going to have to really be constantly vigilant,” Weisman said. “Basically once the information is out there, really the best you can do is constantly monitor.”

Lucky me. I can only hope the scammers will move on to someone else, and Weisman says there is a good chance of that.

“Very often they go for fresher found personal data just because those people are going to be less vigilant, but this is just something that you’re going to have forever. You just have to be eternally vigilant. If you’re not the low hanging fruit, they’ll abandon you because there’s plenty of low hanging fruit out there.”

Let’s hope so.

Tiffani Sherman is a Florida-based freelance reporter with more than 25 years of experience writing about finance, health, travel and other topics.