Hackers Tried to Get 5 Credit Cards, 3 Loans and Unemployment With My ID

thepennyhoarder.com/debt/how-to-prevent-identity-theft-2

February 18, 2021

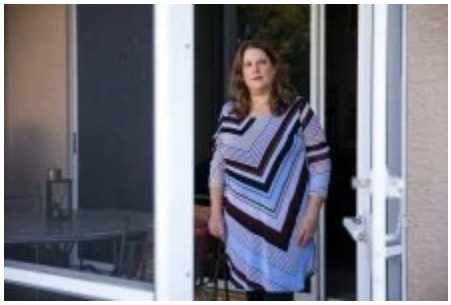
see more from Debt

by Tiffani Sherman

Contributor

5 Hours Ago

Reviewed by Robin Hartill, CFP®



My name is Tiffani Sherman. The real Tiffani Sherman. Not the one who recently applied for unemployment benefits, an SBA COVID loan, five credit cards, a payday advance, two loans, and opened two bank accounts.

That wasn't me.

It also wasn't me back in early 2019 who ordered a bunch of expensive stuff online and then changed the shipping addresses, drained rewards points accounts to buy gift cards, hijacked Amazon and eBay accounts, and monitored and deleted emails for weeks.

For the second time in two years, I'm dealing with the fallout of identity theft.

Trust me, it isn't fun.

I'm having to prove I didn't apply for all of these things and that is taking a lot of my time and energy.

I'm not alone, which doesn't make me feel all that much better.

Identity Theft Is Down, but the Damage Is Worse Than Ever

According to the The 2020 Identity Fraud Report by Javelin Strategy & Research released in May 2020, losses from identity fraud totaled $16.9 billion, which was up 15% from the year before.

According to the report, instances of fraud are falling but the damage they are doing is increasing. Thieves are shifting from fraudulent credit card changes to account takeovers. This kind of thing yields more, is more complex to prevent, and takes longer to fix.

Most of the damage happens within a short period of time. The Javelin research says 40% of the activity usually happens within a day.

With my latest go-around, all of the applications were completed within less than 72 hours.

"It's a very rapid period of time because eventually they're going to experience some friction," said John Buzzard, fraud and security analyst for Javelin Strategy & Research. "They have a small working window of time to really do that total takeover."

How Did Scammers Get My Data?

Almost everyone who heard about my ID theft problems asked me how people got my data.

I honestly don't know. I do know I was part of several high profile data breaches, but who knows if that was it or not.

Scamicide founder Steven Weisman, a nationally recognized expert on identity theft, scams and cybersecurity, says most identity theft happens in one of two ways.

The first is when we accidentally give out our data. "We may have clicked on a link in a text message or an email that had keystroke logging malware that stole the information from our phone or our computer or we may have been tricked into giving personal information over the phone to someone," he said.

We all get those calls and emails where the person says they work for a computer giant and noticed a problem with your computer, or they're from the government and they need your Social Security number. Some of them can sound pretty ominous, so it's easy to fall for them.

Also, think about how many places ask for information like your Social Security number and date of birth.

"Just because somebody asks you for information, that doesn't mean you have to give it to them and that's just something people don't understand," Buzzard said.

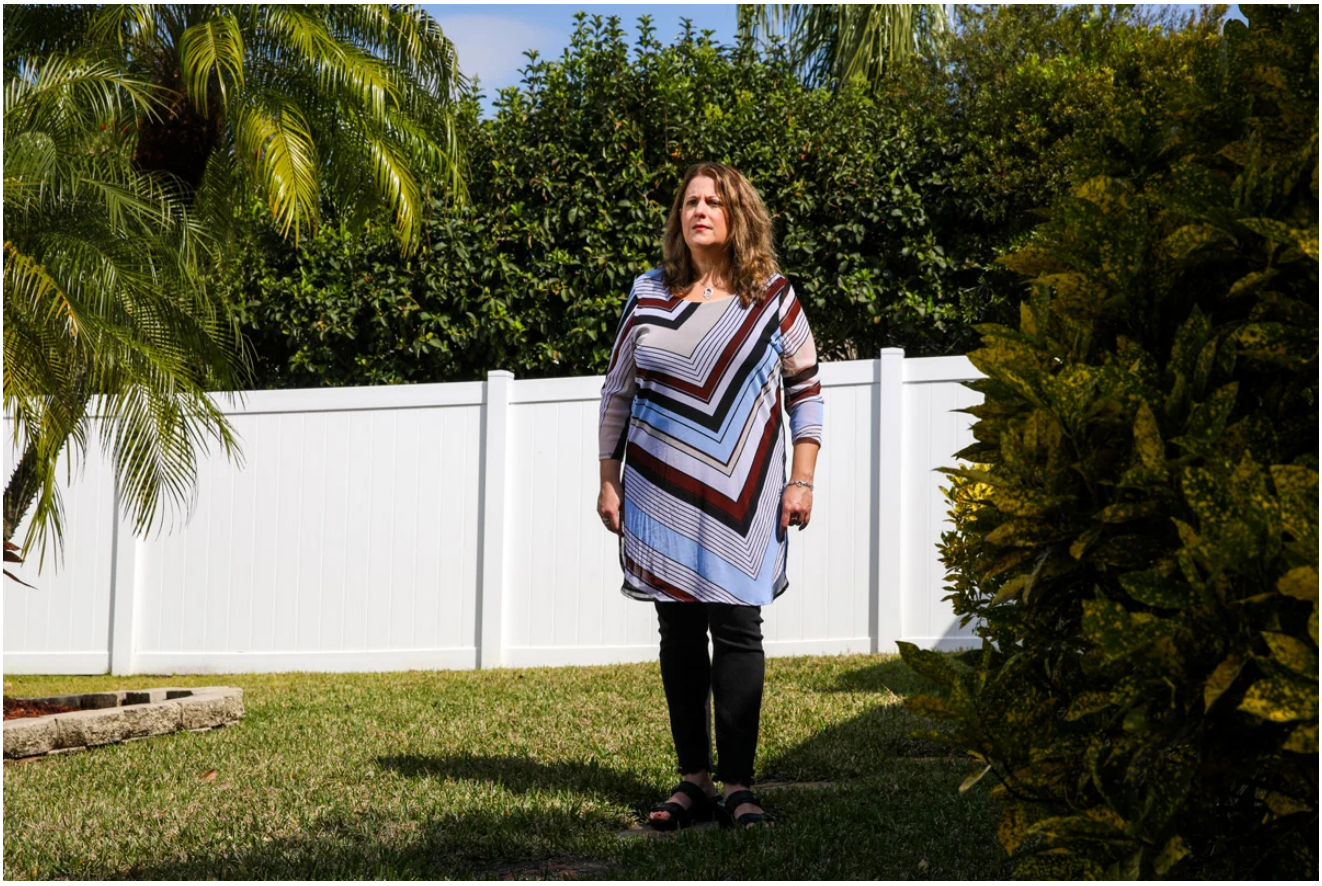
Recently, a grocery store employee asked for his Social Security number when he applied for a store rewards card. "I said, no, I'm sorry. You can have my cell phone number if you need an identifier. If you need a Social, we're done here. You're a grocery store, not exactly a high level security operation. The person folded, put in my cell, and off I went with my rewards card."

The other way scammers get your data is through hackers.

"No matter how good you are at protecting your personal information we're only as safe as the places with the weakest security," Weisman said. "With so many people working remotely these days, people are going to be hacked at home and then through them, [hackers] will get at the networks of the companies for which they work. I think we're going to have a massive amount of major data breaches."

Then the information becomes like pieces of a puzzle.

"It's like a patchwork quilt," Buzzard said. "You pop somebody's information in and you play around with it."



Sherman doesn't know how scammers got her data. Recommended ways to protect yourself from identity theft include setting up alerts, checking your monthly billing statements and using digital wallets. Chris Zuppa/The Penny Hoarder

7 Ways to Make It Hard for Scammers to Use Your Data

Since much of this is basically out of our control, there are some things you can do to make it a bit more difficult for a scammer to use your data if and when they get it.

1. Protect Your Credit

Thieves make easy money with your credit either by charging things on existing cards or opening new credit cards. Either way, they charge a bunch and leave the unsuspecting victim with the bill and damage to their credit.

Even though you're not responsible for fraudulent charges on your credit cards, the hassle you go through to remove the charges is worth taking steps to prevent it.

- **Check your bills:** Look at monthly statements and report any charges you do not recognize.

- **Set up alerts:** Most credit card companies let you set up text or email alerts whenever your card is used. If an alert every time is too much, you can often change the settings to let you know if a card is used without the physical card being present, or if a charge is higher than a certain amount. I've received several notifications that have let me know someone was up to no good, and I was able to quickly report it and cancel the cards.
- **Remove saved payment methods:** I know it's convenient to not have to type in your credit card every time you order something, but having a saved payment method makes it easy for someone who gains access to an online account to do a lot of damage very quickly. This is what burned me in 2019 when someone gained access to my Amazon, eBay and other accounts and bought several things using my card.
- **Use digital wallets:** This type of technology uses encrypted and tokenized data so if someone steals it, it is worthless to them.

2. Freeze Your Credit

Both Weisman and Buzzard said the most important thing to do is freeze your credit. Doing this should stop anyone from opening credit accounts using your information.

When someone wants to open a credit card or get a loan, the institution needs to check the applicant's credit history to know if they are worth the risk or not.

When you have a credit freeze, nobody can access your credit history, so financial institutions will not be able to get the information they need to open an account. This becomes important when a scammer tries to use your personal information to open a fraudulent account. The freeze will automatically stop the account from being opened.

If you want to legitimately open a line of credit, all you need to do is temporarily unfreeze your credit. Just remember to freeze it again.

Each bureau operates separately, so freezing one does not freeze them all, as I found out the hard way. After my issues in 2019, I thought I had frozen all of my credit, but it turns out everything was not frozen. That's how the scammers were able to do so much damage this go-around.

I think it should be easier to freeze your credit and protect yourself from identity theft. Weisman agrees. However, the bureaus make money by gathering your information and selling it to lenders.

"If you freeze your credit, [the bureaus] can't sell the access to your credit," Weisman said. "Freezing your credit makes you less valuable to the credit reporting agencies."

Since Equifax had a huge breach a few years ago, freezing and unfreezing credit is free.

Everyone's credit is separate, so a couple needs to each freeze their credit individually. Freezing one does not freeze the other's. Also, parents can freeze the credit of their minor children.

Even with your credit frozen, check each bureau's credit reports periodically to make sure nothing has gotten through. Also, check to make sure everything is still frozen.

3. Protect Passwords and Personal Information

Part of my problem in 2019 was that someone got hold of several of my passwords, including the email account I used for most of my logins and online commerce. I admit, at the time I was less than vigilant about having a different password for anything and everything. Trust me, that has changed.

As I said, lots of my information including several website and password combinations were part of several well-known data breaches that have happened during the past few years. During these breaches, fraudsters hacked into databases and got the info.

Then they sold that information on the dark web or in other ways. One of those other methods is something called a combolist service (CaaS), which is increasing in popularity. People pay a monthly fee for lists of updated and stolen credentials and personal information that is accessible in the cloud.

I looked and lots of my information is unfortunately part of these combolists.

Once the information is out there, it's impossible to remove it, so all you can really do is change your passwords and keep changing them regularly.

If you forget a password, you can usually reset it by answering some security questions. These present their own set of problems because often the answers are things people can easily find out about you.

"The easy way around this is there is absolutely no rule that says you have to answer your security questions honestly," Weisman said. "You can have really what seems like vulnerable security question like my banks, which is what's my mother's maiden name, but I can put down that my mother's maiden name was firetruck or grapefruit, or something equally ridiculous. And the good thing there is, you will remember that security question, because it's just so ridiculous and no one is ever going to be able to crack that."

As for those password vaults, security experts are mixed about them. One remediation expert I talked with to help me with my issues said she doesn't like them because if someone breaches the vault, they have access to everything. Other people say they are a good way to make sure you have strong passwords for everything.

4. Don't Give Out Information on Social Media

I just saw a post on a friend's social media page saying the song that was most popular the week you turned 14 defines who you are. It also defines the year you were born to any online scammer who is looking for that important piece of information.

The same goes for quizzes that talk about favorite pets, first cars, favorite teachers, school mascots, etc. Seeing those types of things now makes me cringe. Many people are making it way too easy for scammers.

5. Enable Two-Factor Authentication

Enabling two-factor authentication is also important. If someone tries to log into your account, the vendor will send a one-time code either to the email address or phone number on file.

"Data breaches will happen," Weisman said. "People will make mistakes and fall for a spear phishing email and suddenly they may have had their usernames and passwords turned over. So you always want to have dual factor authentication whenever you can so even if someone has your username and password, they can't access your account."

Just make sure you protect your phone also by enabling its security features.

To save you the hassle of having to receive a code each time you want to log into your own accounts, some websites will allow you to save devices so the next time you log in, it will remember that device's IP address and allow the login without the extra security.

Be wary of any email, phone call, or text you receive saying something has been compromised and to click on a link or call a number to reset it. Instead of clicking on the link, go to the website or app itself and reset the password directly from there.

6. Secure Devices

We live for our devices. They're our constant companion and contain our whole lives. Protect them.

- **Update operating systems and security software:** Companies issue updates once they identify a vulnerability a hacker could exploit. Sadly, this isn't always foolproof. "Even if you get the most up to date security software, it's always going to be about a month behind the latest what we call zero date defects," Weisman said.
- **Install malware protection:** Malware is short for malicious software and it is basically anything that can harm or exploit a device. There are many different kinds. Often, it finds its way on to our devices because we click on a malicious link or open an attachment that unleashes the software. Don't forget to protect your phone.

- **Secure Wi-Fi connections:** Make sure you secure your wireless router and change the password on it.
- **Secure IoT items:** It's true. Your refrigerator may be spying on you. Many things in your home connect to the internet and can provide access to your network and other items on it which can contain personal information.

Weisman suggests taking one more step to secure your phone which is locking your number. This way, a scammer can't transfer your phone number to another carrier.

Think about it. With many two-factor authentication codes coming to your phone, if someone had your personal information AND took control of your phone number, you wouldn't get your codes. They would.

Locking my number was easy to do from my provider's app. If I ever want to change cell providers, I can use the app to create a temporary PIN to allow the change.

7. Don't Rely on Protection Services

There are many services out there that say they will protect you from identity theft.

Weisman is not a huge fan because they don't usually protect you. They just alert you sooner.

"I liken them to crossing a street and I get hit by a bus and someone runs out into the street and tells me, 'Hey you just got hit by a bus,'" Weisman said. "That's what the identity theft protection services are doing. They're telling you sooner that you've been victimized. They don't do anything to protect you from becoming a victim."

Since most of the personal information out there comes from data breaches, phishing emails, etc., it isn't possible to totally prevent the theft of personal information. The best we can do is attempt to control what the scammers can do once they get it.

My friends keep asking me if I stopped everything. Sadly, I cannot answer that question. The flurry of attempts to open new accounts seems to have calmed for now, but I'm waiting for the next round.

It's a helpless feeling.

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