The Very Best Ways to Prevent Credit Card Fraud

You can reduce your risk for credit card fraud with good credit card safety habits.

By Beverly Harzog

March 3, 2021, at 9:33 a.m.

Credit card fraud was the most frequent type of fraud reported in 2020, according to the Federal Trade Commission. The total loss due to credit card fraud? A whopping $149 million.

While it's important to know what steps to take if you're a victim of credit card fraud, practicing credit card safety from the moment you get a new credit card can go a long way toward credit card fraud prevention.

Let's take a look at what you'll learn ahead:

- Credit card fraud vs. identity theft.
- How to prevent credit card fraud.
- Make credit card safety a habit.

[

READ:

Best Rewards Credit Cards.]

Credit Card Fraud vs. Identity Theft

The two are similar, but identity theft is broader in reach. A thief who steals your identity might use your personal information, such as your Social Security number, to open a new credit card account, get a loan or even file taxes in your name.

Credit card fraud is a form of identity theft that happens when your account is used for unauthorized purchases. For instance, when you check your credit card account online, you might notice that there are purchases that you didn't make. Although many of the major card issuers offer zero liability on fraudulent purchases, it's still your responsibility to be on the lookout for fraud and to report suspicious transactions as soon as possible.

There's no foolproof strategy that gives you total credit card fraud protection, but since some everyday actions can increase your fraud risk, it's worth your time to learn how to practice credit card safety.

How to Prevent Credit Card Fraud

There are a variety of ways that scammers try to fool you or steal your information. Fraud reports for 2020 increased over the previous year, which isn't surprising given the pandemic. During a crisis, fraud tends to increase. The perpetrator is hoping to catch you at a vulnerable moment.

Sometimes, just being aware of what to watch out for can help you make better decisions and avert credit card fraud. Let's take a look at some simple ways to prevent fraud:

- Don’t use unsecure websites.
- Beware of phishing scams.
- Be on the lookout for skimmers.
- Don’t post sensitive information on social media.
- Get comfortable with mobile payment apps.
- Shop in stores that have chip readers.
- Don’t save your credit card information online.
- Use a virtual credit card number online.
- Use a password manager.
- Get a chip card with PIN capacity.
- Don’t trust public Wi-Fi for financial transactions.
- Set up a fraud alert or credit freeze if your card is lost or stolen.
- Review your credit reports regularly.

Don’t use unsecure websites.

Let's start with something basic that's really easy to do. If the site is secure, you'll see a padlock on the left side of the address bar at the top of your browser.

Also, the web address will begin with HTTPS. Do not enter your credit card number on a website that isn't secure. And let's be honest, if a business isn't offering data security for its customers, it doesn't deserve your business.

Beware of phishing scams.

These scams can happen by phone, email, text or even snail mail. The objective is to get you to hand over your financial information. The scammer might call and pretend they are from an institution you trust, such as a bank or the Social Security Administration.

I recently got a call from the SSA and was told I needed to confirm my Social Security number to keep getting Social Security checks. First, I don't get Social Security checks. But since I knew this was a common scam, I was suspicious from the start. The caller ID even showed the call was from the SSA.

Today's scams are technically sophisticated. You might get an email with what appears to be your bank's logo, and you might assume it's legitimate. If the email requests you reply with your credit card account number, you know it's fake.

A government or financial institution will never ask you to give sensitive information that way. One way to spot these scams is if you see typos in the communication. Thieves can be clever, but they often can't spell correctly.

Be on the lookout for skimmers.

Credit card thieves often use a device called a skimmer to steal your credit card information. They try to hide these devices on ATMs and fuel pumps and "skim" the data from the magnetic strip on the back of your credit card.

Whenever you pay for gas at the pump or use an ATM, look for signs of tampering. If you're unsure at all, pay for your gas inside the store. If it's an ATM that looks altered, find another ATM that's affiliated with your bank. And, of course, use your EMV chip credit card if you can, though not at an ATM. Not only do credit card issuers typically charge higher interest rates on cash advances, but they also typically start charging interest immediately with no grace period.

Don’t post sensitive information on social media.

If you think this doesn't need to be said, spend a few hours on any social media platform. And if you have older kids online, give them a serious talk about this. Thieves comb through social media looking for clues that they can piece together about your life and your financial data. Tip: Don't use your pet's name for a password.

Get comfortable with mobile payment apps.

Your credit card information is less likely to be skimmed at an in-store card reader, but the threat still exists. Increase your credit card fraud protection by using mobile payment apps, such as Apple Pay, Samsung Pay or PayPal.

These apps use a technology called tokenization, which allows you to pay without exposing your actual credit card account number. So even if your transaction information falls into the wrong hands, your actual account number remains safe.

[

READ:

Best No-Annual-Fee Credit Cards.]

Shop in stores that have chip readers.

Using an EMV chip card offers some protection because it isn't easy to clone these cards. There are still retailers that only have magnetic-strip cards. But if possible, try to limit your purchases to stores that accept chip cards.

As I mentioned with skimmers, chip cards have an extra layer of fraud protection. Do keep in mind, though, that when you shop online, that extra protection doesn't exist. This is called card-not-present fraud because you're giving the site your credit card account number but you're not using the chip technology. Online you don't have the benefit of the chip-enabled security that occurs when you use your card in person.

Don’t save your credit card information online.

I know this is a tough rule to follow because it takes time. You have to stop, find your credit card and type in the account number. Even with retailers you trust, a data breach can occur, so it's not a good idea to store your account information on a website. But if you can handle typing in your card account number each time, it's an effective way to decrease your fraud risk.

Use a virtual credit card number online.

This feature isn't offered by many issuers, but if your issuer does, take advantage of virtual numbers. Here's how it works: Through your issuer's tool, you can request a virtual credit card number to use online. You'll get a unique virtual account number to make a purchase instead of your actual credit card number.

Since your chip credit card doesn't give you extra protection online, a virtual credit card number helps boost credit card fraud protection. If the retailer suffers a breach, your actual credit card number is safe.

Use a password manager.

One of the rules with using passwords is that you should refrain from using the same password across multiple sites. If a thief gets hold of one of your passwords, say for your credit card account, the thief will try that password on your checking account.

See the problem? And yes, keeping track of all of your complicated passwords is a pain, for sure. That's why you should use a password manager. There are some excellent password managers, such as Bitwarden and LastPass, that come free or with upgraded paid accounts.

Get a chip card with PIN capability.

Most credit cards in Europe come with a chip and PIN feature, but few card issuers in the U.S. have followed suit. Without a PIN, you'll not only have a difficult time using automated kiosks overseas, but you may also be exposed to potential fraud.

[

READ:

Best Starter Credit Cards for Building Credit.]

Don't trust public Wi-Fi for financial transactions.

If you disclose your credit card number or bank account over public Wi-Fi, you'll be vulnerable to hackers because these networks are often unencrypted. Thieves may be lurking in public areas waiting to catch someone off guard and steal their information. Whatever financial moves you need to make, wait until you're on a secure network.

But this doesn't mean you have to avoid public Wi-Fi altogether. You can use a virtual private network, or VPN, to keep your information safe from crafty eavesdroppers.

Set up a fraud alert or credit freeze if your card is lost or stolen.

As soon as you realize your credit card is gone, report this immediately to your credit card issuer so it can freeze your account.

If you aren't sure how long your card has been missing, the safest thing to do is set up a fraud alert or a credit freeze. With a fraud alert, when a thief tries to open an account, the creditor will typically call you to verify your identity and confirm that you were the one who applied. With a credit freeze, creditors can't even access your credit reports, making it impossible for them to approve a credit application by an impostor.

Review your credit reports regularly.

You get a free annual credit report every 12 months from each of the three major credit bureaus: Equifax, Experian and TransUnion. You need to review your reports at least annually to make sure all is in order.

For starters, you want to make sure all the data in your report are accurate. If there's a big error, it's possible it will have a negative impact on your credit score. You also want to make sure that you don't see new accounts that you didn't open. If you do, this is a sign of credit card fraud and possible identity theft. You'll need to take steps to report the fraud as soon as possible.

Make Credit Card Safety a Habit

It's true that you could be diligent about credit card fraud prevention and still be a victim of fraud. But by doing everything you can to thwart it, you will have reduced your risk quite a bit.

Your last step for credit card prevention: Check your online financial accounts several times a week. Look for signs of fraudulent purchases and report them immediately. If you find fraud early, you'll go a long way toward minimizing the financial – and emotional – damage.