ACCOUNTING & AUDIT

Credit Card Fraud Has Spiked During Pandemic

Overall, most consumers reported higher losses of money as their age increased. Those between the ages 30-39 reported an average of $379 lost, versus $1600 lost from those 80 years and older. These numbers may not seem like much, but they ...

Sep. 01, 2020

With fraud numbers rising dangerously high during the ongoing pandemic, further security precautions are necessary as businesses and tax professionals move forward. Every day we see more and more situations in which money is taken or identities are stolen.

The FTC Study

The FTC recently released its findings on the fraud environment during the pandemic. The statistics are frightening. Credit card fraud has seen unprecedented growth in recent months and is one of the fastest-growing forms of identity theft. Reports of credit card fraud jumped 104% from 2019 to early 2020. To put this into perspective, from 2017 to 2019, there was a 27% increase in reported fraud cases, marking a major difference.

Luckily, the FTC was able to return $232.3 million to victims of identity theft and fraud during 2019 alone. Though this is a major win for consumers, it's only a fraction of the money that was actually taken by scammers.

Different demographic variables, such as age, also revealed how fraudsters approach certain types of victims. For example, those aged 20-69 reported more internet-based

fraud. Victims aged 70 years and older, however, were contacted via phone.

Overall, most consumers reported higher losses of money as their age increased. Those between the ages 30-39 reported an average of $379 lost, versus $1600 lost from those 80 years and older. These numbers may not seem like much, but they focus solely on the consumer side of losses, excluding losses from financial institutions and other parties.

Staying Safe from Fraudsters and Scammers

Credit Card Insider recently analyzed the FTC survey and concluded that further education is essential. The more you know about how fraud works and how it can be avoided, the better you can protect yourself both in professional and personal situations.

You'll first want to make sure you're familiar with the basics of fraud and scams, and what thieves look for. Most scammers try to get as much confidential information about you as they can, especially your Social Security number, annual income, cost of rent or mortgage, birthday, and even your card PIN numbers. This information is commonly needed when applying for new accounts, lines of credit, and other financial products.

Learn What to Avoid

Phone Scams: Phone scams are very common, especially for older individuals. Phone scammers usually focus on creating a sense of urgency, perhaps by imitating a government collection agency or your financial institution, in the hopes of scaring you into paying to avoid a problem. If you experience a call like this, especially if it's a "robocall", hang up, and call your financial institution to learn more about the possible problem.

Phishing: Phishing is a fairly well-known scam where you're typically contacted via email from someone impersonating a company or agency. Again, the sender will ask for your personal and payment information in order to avoid an urgent problem. If it looks like you've received a phishing email, don't open it. If you do, NEVER click on links within the email. They may contain viruses and malware that can damage your phone or computer.

Skimming

Thieves often attempt to tamper with in-person forms of payment by placing skimmers in terminals at stores, ATMs, or gas pumps. A skimmer is a device that can read your credit card information so a thief can use it for their own purposes. If you notice anything unusual while at an ATM or gas station, such as a loose credit card reader, DO NOT insert your card and report the problem immediately.

Shimming

Shimming is similar to skimming, except shimming devices are designed to steal information from chip cards rather than magnetic stripe cards. Again, if you find that a point-of-sale terminal or another form of payment technology has been tampered with, avoid it and report it to the proper authorities.

Ways to Protect Yourself

- **Use a credit card rather than a debit card.** Most include a $0 liability policy, which generally makes it easier to dispute charges and recover your money. Plus, even if you do fall victim to fraud, it's the issuer's money that's on the line — not your own.
- **When possible, use mobile wallets or contactless cards.** These technologies require no physical contact, which makes it harder for hackers to steal your information during in-person purchases.
- **NEVER exchange information with unverified parties.** If you receive a phone call or email from an unsolicited source and they ask for your information, DON'T give it to them, and do your research to verify their authenticity. Then, find their official contact information and reach out yourself. If the exchange requires you to provide sensitive information, try to make it happen in person — by visiting a brick-and-mortar bank branch, for example.

======

Mason Miranda is a Credit Industry Specialist at Credit Card Insider. Mason fights to help others live their values in their financial circumstances. His passion is informing communities on best practices for eliminating debt, improving financial management, and adopting habits for success. He believes that true success starts with your mindset and continues with action.

CPAPA is registered with the National Association of State Boards of Accountancy (NASBA) as a sponsor of continuing professional education on the National Registry of CPE Sponsors.