Protecting Your Finances

Five Ways To Fight Back Against Identity Fraud

(NAPSA)—If you've been a victim of identity fraud lately, you're not alone. Nearly 17 million other Americans were, too, according to the 2018 annual Identity Fraud Study released by Javelin Strategy & Research, a research-based advisory firm that helps its clients to make better-informed business decisions in a digital financial world. In 2017, fraudsters stole $16.8 billion in the U.S. alone, the Javelin study found.

Identity fraud is defined as the unauthorized use of another person's personal information to achieve illicit financial gain. It can range from simply using a stolen payment card account, to making a fraudulent purchase, to taking control of existing accounts or opening new accounts.

The study identified four significant trends:

• Record high incidence—In 2017, 6.64 percent of consumers became victims of identity fraud.

• Total account takeover losses reached $5.1 billion. Account takeover continues to be one of the most challenging fraud types for consumers, with victims paying an average of $290 in out-of-pocket costs and spending 16 hours on average to resolve.

• Online shopping presents the greatest fraud opportunity. Card-not-present fraud is now 81 percent more likely than point-of-sale fraud.

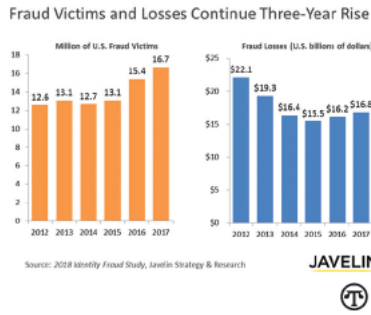
• Fraudsters are getting more sophisticated. One and a half million victims of existing account fraud had an intermediary account opened in their name first.

Five Safety Tips To Protect Your Identity

Fortunately, you can protect yourself. Here are some tips on how:

1. Turn on two-factor authentication wherever possible—Enabling two-factor authentication, where a separate action must be taken beyond providing a user name and password to access an account, can make it significantly more difficult for fraudsters to take over your accounts. Also, use strong passwords or a password manager to secure accounts.

2. Secure your devices—Criminals have shifted their focus to digital devices for the access they can provide to accounts and the information they store or transmit. Institute a screen lock, encrypt data stored on the devices, avoid public Wi-Fi, use a VPN, and install anti-malware.



Identity fraud is up but you don't have to let it get you—or your finances—down.

3. Place a security freeze—If you're not planning on opening new accounts in the near future, a freeze on your credit report can prevent anyone else from opening one in your name—especially important if a data breach has exposed sensitive, personally identifiable information. Credit freezes must be placed with all three credit bureaus and prevent everyone except existing creditors and certain government agencies from accessing your credit report. Should you need to open an account requiring a credit check, the freeze can be lifted through the credit bureaus.

4. Sign up for account alerts—Many financial service providers, including depository institutions, credit card issuers and brokerages, as well as e-mail and social media providers, offer the option to get notifications of suspicious activity. Some even let you specify the scenarios under which you want to be notified, to reduce false alarms.

5. Protect yourself from unauthorized online transactions—Embedded chips make fraud at physical stores more challenging, so fraudsters target online merchants. Some financial institutions offer alerts for online transactions, the ability to institute limits on online transactions, or even advanced controls through 3-D Secure (for example, Verified by Visa, SecureCode from Mastercard, and others). These can help quickly detect and even prevent online fraud from occurring.

Learn More

For other ways to protect yourself, visit www.identityguard.com/news-insights. To report incidents of suspected fraud or identity theft, visit the FTC at www.ftc.gov/faq/consumer-protection/report-identity-theft.