2020 Javelin Identity Fraud Study FAQ

JAVELIN

1. The key findings of the annual report identify a major shift in how criminals are stealing and indicate that companies do not have the technology in place to prevent the fraud from escalating.

Fraud loss rates increased by 13% in 2019, 5.08% of consumers experienced identity fraud. As criminals focus more intensely on a smaller number of victims they maximized the value gained from each victim, increasing the total loss for each fraud type. Overall losses rose by over $2 billion to $16.9 billion in 2019.

Account takeover (ATO) is the new normal. Even as other fraud types remained steady or fell from 2018, account takeover grew from 3.6 million victims in 2018 to 4.4 million in 2019. Losses for ATO schemes saw the sharpest increase, growing 72% to reach $6.8 billion in 2019, or 42% of losses from fraud schemes targeting existing accounts.

New-account fraud has transformed. Credit cards have been dethroned as the most prevalent target for fraudulently opened new accounts. In 2019, both general online accounts outside of financial services and new checking and savings accounts topped general purpose credit card accounts as the most common NAF targets. This reflects the new reality that fraudsters have a growing array of options for how to monetize

Although there were fewer fraud victims in 2019, this does not mean consumer out-of-pocket cost was any lower. The cost of mitigating identity fraud in 2019 increased to 26% as consumers continue to pay for out-of-pocket costs related to identity fraud.

2. The COVID-19 pandemic is expected to increased specific types of fraud as criminals take advantage of the changing market dynamics.

Card not present fraud was 3.1% compared to point of sale fraud rates of 1.2% in 2019. Card not present fraud, phishing attacks, scams, and full account takeover fraud should be anticipated. Consumers, retailers, and financial institutions need to ensure that added monitoring is in place to minimize losses.

3. Consumers can take active steps to prevent identity fraud from impacting their lives.

Changing existing behaviors in how people use payments and make purchases will help in keeping their financial lives healthy. The following are recommendations for consumers to follow:

a. Use digital wallets to manage in-store and online payments. The technology encrypts and tokenizes data so if it is stolen it is useless information to the criminals. Added benefit of using tap and go payments like digital wallets and contactless cards means that there are also fewer health implications when making payments in person.

b. Consumers need to adopt a zero trust contact policy. There are so many socialized scams today that leverage one-time passcodes and fraud verification services in order to perpetrate payment fraud and account takeover fraud. Most consumers fail at questioning the authority and authenticity of a text or caller and the damage can be rapid and costly. The only acceptable action when receiving unexpected contact with a potential imposter is to exhibit zero trust. The new mantra? "Hang up and call your financial institution."

c. Turn on two-factor authentication wherever possible – but guard the one-time passcodes closely by not divulging them via text or phone call. Enabling two-factor authentication on sites that have that capability is a great idea, but it can be one rife with threat when a fraudster attempts to steal your password and one-time secondary passcode. For sites without two-factor authentication, use strong passwords or a password manager to secure highly complex and varying passwords on accounts.

d. Secure your devices. With consumers increasingly relying on their digital devices to access financial services, make purchases and share personal information, criminals have shifted their focus to these devices for the access they can provide to accounts and the information they store or transmit. Consumers should secure online and mobile devices by instituting a screen lock, encrypting data stored on the devices, avoiding public Wi-Fi and/or using a VPN, and installing anti-malware. Anti-malware protection is essential for all devices.

e. Place a security freeze on credit reports. Placing a freeze on your credit reports can prevent anyone else from opening one in your name and there is no cost to initiate. This security measure is especially important if you have been a victim of a data breach that has exposed sensitive, personally identifiable information. Credit freezes must be placed with all three credit bureaus and will prevent anyone except for existing creditors and certain government agencies from accessing your credit report. Should you need to open an account requiring a credit inquiry, the freeze can easily be lifted for up to 90 days or more through the credit bureaus websites and or smartphone apps.

f. Sign up for account alerts everywhere. A variety of financial service providers, including banks, credit card issuers and brokerages, provide their customers with the option to receive notifications of suspicious activity – as do businesses in other industries, such as email and social media providers. These notifications can often be received through email or text message, making some notifications immediate, and some go so far as to allow their customers to specify the scenarios under which they want to be notified, so as to reduce false alarms.

g. Can your financial services provider easily locate and contact you? Consumers often forget to update new addresses and phone numbers with their financial institutions and lenders. Payment cards are so popular today that they continue to work as long as there are funds to support them and this usually translates into a disconnect between the consumer and the provider when valuable information has to be exchanged via U.S. mail, email, or voice communication. Remember: You cannot receive a fraud alert if your new cellphone number hasn't been updated.

4. What is identity fraud?

Identity fraud is defined as the unauthorized use of another person's personal information to achieve illicit financial gain. Identity fraud 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.

5. How is identity theft different than identity fraud?

Identity theft is defined by Javelin as unauthorized access of personal information. It can occur without identity fraud, such as through large-scale data breaches. Once the theft is coupled with illicit financial gain, then Javelin considers it identity fraud.

6. Why are victims paying losses out of pocket?

Criminals are actively taking over accounts and causing greater financial damage in each event. When a checking account is taken over, consumers may be responsible for bounced check fees and over limit fees at locations they pay their bills. Add in the need to hire attorneys, pay for insurance, and credit monitoring capabilities, consumers are increasingly impacted when account takeover and new account fraud occurs.

Consumers also need to be mindful of person-to-person (P2P) payment fraud. When a consumer is scammed into sending money, for example purchasing COVID-19 prevention kits, the consumer is responsible for the fraud, which occurs because they did send money. Consumers captured in scams do not have fraud protection from the financial institution and funds are irrevocable.

7. What is Account Takeover?

Account takeover is when a criminal is able to gain access to a consumer's online account and then proceeds to change login or contact information to assume control of the account and prevent the legitimate owner from receiving alerts and regain control of the account. In 2019, 53% of all existing account fraud is from account takeover.

8. What is New-Account Fraud?

New-account fraud (also known as application fraud) is when someone fraudulently opens a new account in the victim's name. Fraudsters are always looking for ways to access victims' information and are finding new vulnerabilities, such as new-account fraud. By opening a new credit card account, for example, fraudsters can prevent their victim from seeing fraudulent transactions on their monthly statements. This provides fraudsters with more time to cultivate higher credit limits for lucrative payouts.

9. What is Identity Proofing and why is it an important factor in curtailing identity fraud?

Counterfeit forms of ID are plaguing business enterprises across the U.S. today. Financial institutions and lenders are often presented with counterfeit forms of ID on a daily basis as criminals attempt to open new accounts and loans using synthetic or stolen identities. The potential for financial loss is considerable. Identity Proofing ensures that a state-issued ID or passport is not counterfeit. Simply relying on authentication methods (like challenge questions) is simply not an adequate means to reduce ID fraud at the enterprise level.

10. What is it going to take to see substantial progress in the reduction of identity fraud?

To reduce identity fraud, consumers, businesses, and financial institutions need to change the bad habits of using outdated security measures. Simple changes will make a big difference. Use contactless cards, watches, and fitness bands. Use digital wallets in-store and online. Use biometrics when possible and two factor authentication. Stop using static passwords. Incorporate various data points into a stronger authentication protocol.

11. How can consumers find and detect fraud?

There are a variety of digital tools that consumers can leverage to stay informed about the status of their accounts (like account alerts). The easiest method of detecting anomalous account activity is to simply review account activity on a daily or weekly basis. It is essential for consumers to report unusual transactions to their service providers as soon as possible to avoid additional losses or penalties in resolving suspected fraud activity.

Consumers are always encouraged to visit the Federal Trade Commission (FTC) website if they wish to self-educate or file identity theft reports. To report incidents of suspected fraud or identity theft, visit the FTC online at www.ftc.gov/faq/consumer-protection/report-identity-theft.

12. If consumers become victims, what should they do?

Consumers who think they are a victim of identity theft should take the following suggested actions:

a. If any existing accounts were misused, notify your account providers.

b. Ask your financial services provider or business partner if they require a police report or signed affidavit in order to process a fraud claim. Make sure that you save a copy of all documentation for your records and make every attempt to maintain a record of each action you take to mitigate the problem, complete with dates, times, and out-of-pocket costs.

c. Place an "alert" at all three credit bureaus (Equifax, Experian and TransUnion) and take the time to enable a credit freeze at each credit bureau. Close any unauthorized accounts immediately. Request a free copy of your credit report directly from the credit bureau. Every U.S. consumer is entitled to one free annual credit report.

d. Consider enrolling in monitoring/alert services to track any changes to your credit, addresses or public records, and be vigilant. Public record information will not show up on a credit report and can be used to commit fraud. Check our sponsors' websites for fraud prevention information and solutions.

e. Start fresh with new payment card numbers, user logins, and passwords. Focus on user logins, and passwords that are not specific to your name or personal information. Passwords should be complex and a minimum of 8 characters or more.

f. Maximize the effectiveness of every communication with your financial institutions. It is important to ask how long you have to resolve fraudulent claims. Understanding what items your financial institution covers as "zero liability" may change from year to year, so it's important to determine the scope of what you may be responsible for. Cooperation and timely disposition of accurate documentation is essential to a faster resolution of identity fraud.

13. What is the study's methodology?

In 2019, Javelin conducted a nationally representative online survey of 6,000 U.S. consumers to assess the impact of fraud, uncover where fraudsters are making progress, explore consumers' actions and behaviors and how it relates to fraud risk levels, and identify segments of consumers most affected by fraud.

Now in its seventeenth consecutive year, it is the nation's longest running study of identity fraud, with 85,000 respondents surveyed since 2003. The comprehensive analysis of identity fraud trends is independently produced by Javelin Strategy & Research, and made possible by FIS, a global financial services technology provider.

14. What role did AARP, Allstate Identity Protection, FIS, and GIACT play as sponsors?

This is an independent research and education project made possible with the support of AARP, Allstate Identity Protection, FIS, and GIACT. Javelin worked with the sponsors to gather suggestions for updated consumer survey questions in a few select areas that are subject to the most dynamic fraud trends or changes in consumer behavior. The companies participated in the project as a public education and awareness campaign, and were given no opportunity to influence the data or shape the results of the Javelin report in any way.