JAVELIN

2020 Identity Fraud Study: Genesis of the Identity Fraud Crisis

07 April 2020 By: Krista Tedder, John Buzzard

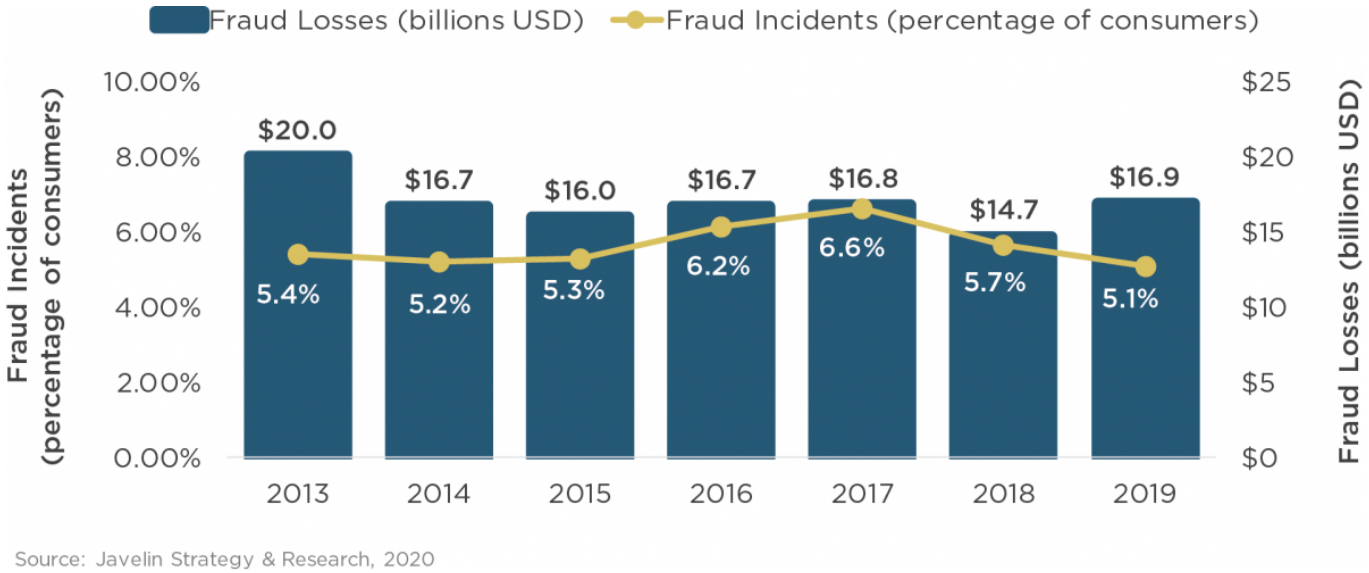
PERMISSIONS AND COPYRIGHT GUIDELINES

Javelin's 2020 Identity Fraud Study provides comprehensive analysis of fraud trends in the context of a changing technological and payments landscape in order to inform consumers, financial institutions, and businesses on the most effective means of security, detection, and resolution.

The comprehensive analysis of identity fraud trends is independently produced by Javelin Strategy & Research and made possible with support from our sponsors. A thank you to our lead sponsors, AARP, Allstate Identity Protection, FIS, and Giact for making this report available to Javelin Advisory Services clients for their internal use only. The study is in its seventeenth consecutive year and is the nation's longest-running study of identity fraud, with 85,000 consumers surveyed since 2003.

OVERVIEW

The results of Javelin's 2020 Identity Fraud Survey serve as a wake-up call—one that will force financial institutions, businesses, and the payment industry to reevaluate how identity fraud is managed. Total identity fraud reached $16.9 billion (USD) in 2019, yet the dollar loss is only part of the story. To have a more fulsome understanding of identity fraud a comprehensive evaluation of the drop in number of victims lead to several unsettling findings. Criminals are targeting smaller numbers of victims and while inflicting damage that is more complex to prevent or remediate.



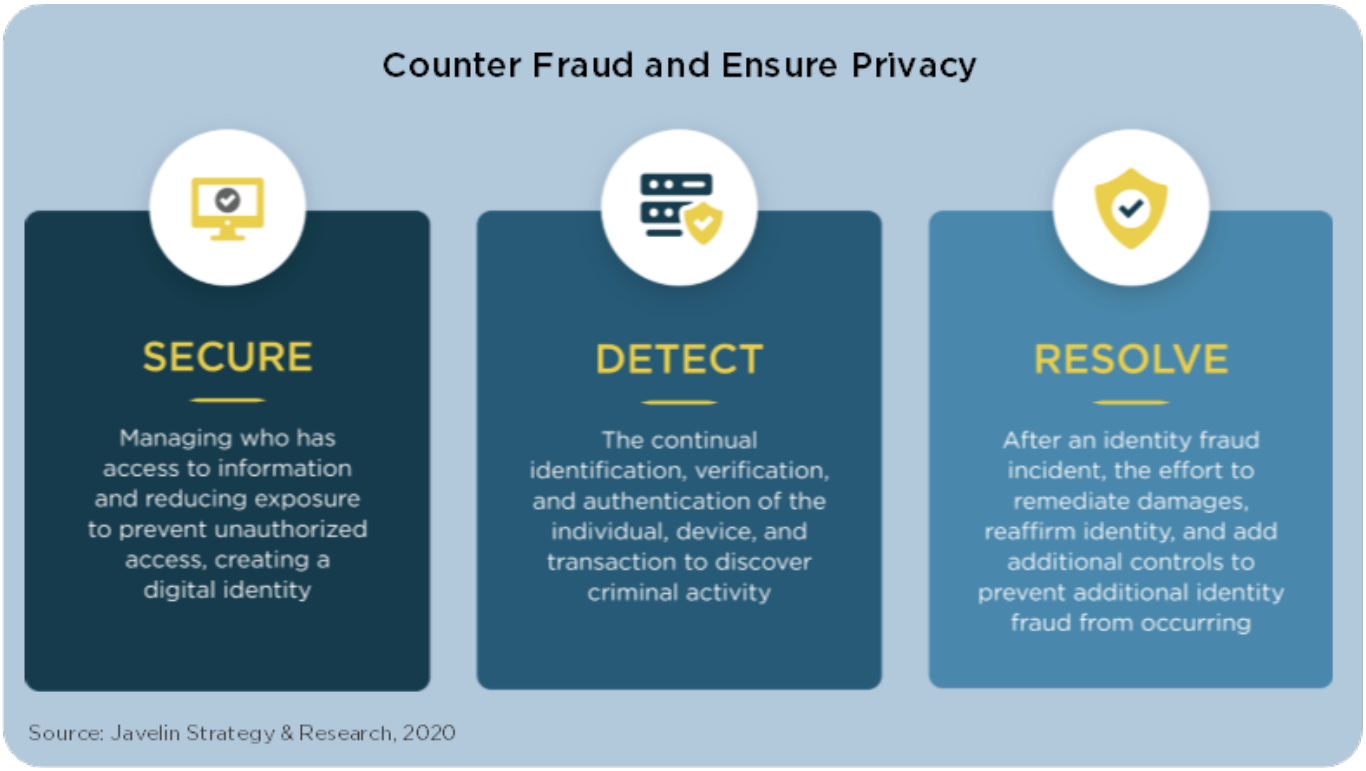
Source: Javelin Strategy & Research, 2020

The type of identity fraud has drastically changed from counterfeiting credit cards to the high-impact identity fraud of checking and savings account takeover. At a time when consumers are feeling financial stress from the global health and economic crisis, account takeover fraud and scams will increase. It is too early to predict how much higher the fraud rates will go; however, criminals become more active during times of economic hardships.

Account takeover fraud is one of the hardest types of fraud to identify because of the multichannel account access and the desire to reduce friction in the consumer experience. New technology is available to help mitigate risk and improve the consumer experience, yet often it goes unused or is unavailable to consumers. What is clear is that criminals are adapting to new technology faster than consumers will adopt technology to reduce their risk.

During the next twelve months, criminals will strike at the heart of the financial services industry and negatively affect consumers. Areas of concern range from fraudulent account openings (synthetic identities), person to person (P2P), and full takeover of all accounts, not just checking or cards but also investment accounts and other high-dollar balances. Criminals will always try to take what isn't theirs, and right now it is too easy. The level of fraud could climb back to pre-EMV levels if steps are not taken to prevent the new identity fraud schemes.

The challenge of reducing fraud losses is not always the lack of technology investment. It can also be the failure to focus on increasing consumer adoption of safer methods of safeguarding their information and managing their finances. To counter fraud and ensure data privacy, the conversation needs to change from monitoring activity that is occurring to securing the information before it is stolen.



CONSUMER RECOMMENDATIONS

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:

1. 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.
2. 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.”
3. 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.
4. 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.
5. 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.
6. 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.

7. 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.

The Javelin Identity Fraud Study provides businesses, financial institutions, government agencies, and other organizations an in-depth and comprehensive examination of identity fraud and the success rates of methods used for prevention, detection, and resolution.

Survey Data Collection

The 2019 ID Fraud survey was conducted online among 5,000 U.S. adults over age 18; this sample is representative of the U.S. census demographics distribution. Data collection took place from October 22 through November 4, 2019. Final data was weighted by Dynata (formerly SSI), while Javelin was responsible for data cleaning, processing, and reporting. Data is weighted using 18+ U.S. Population Benchmarks on age, gender, race/ethnicity, education, census region, and metropolitan status from the most current CPS targets.

In adherence with best practices, in 2011 Javelin also moved from bracketed dollar amount calculations to true open-end numerical dollar calculations. On continuous variables captured from numerical open-ended items, extreme outliers were identified using a standard rule of approximately 2 standard deviations above the mean to retain consistency year over year. These extreme outliers were replaced with mean values to minimize their disproportionate effect on final weighted estimates. Where responses pertained to a range in value (e.g., "one day to less than one week"), the midpoint of the range was used to calculate the median or mean value. To ensure consistency in comparing year-to-year changes, historical figures for average fraud amounts have been adjusted for inflation using the Consumer Price Index.

Due to rounding errors, the percentages on graphs may add up to 100% plus or minus 1%.

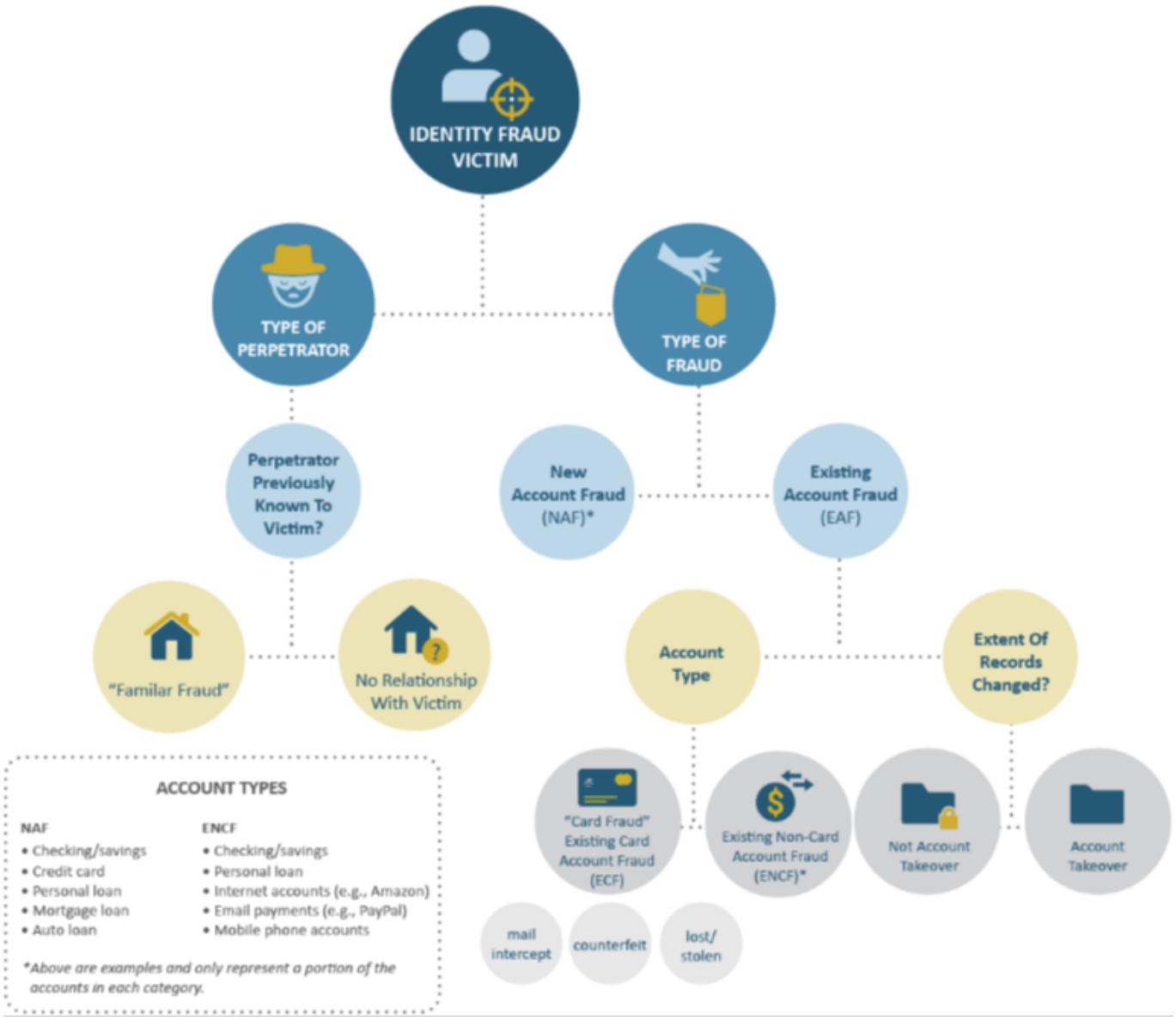
Categorizing Fraud by FTC Methodology

With one exception, this report continues to classify fraud within the three categories originally defined by the FTC in 2003. For 2005 and beyond, debit card fraud has been recategorized as existing card account fraud instead of existing non-card account fraud. Javelin believes this change reflects a more accurate representation of debit card fraud, because much more of its means of compromise, fraudulent use, and detection methods parallel those of credit cards.

The categories of fraud are listed below rom least to most serious:

- Existing card accounts: This category includes both the account numbers and/or the actual cards or existing credit and card-linked debit accounts.
- Existing non-card accounts: This category includes existing checking and savings accounts and existing loans and insurance telephone and utilities accounts.
- New accounts and other frauds: This category includes new accounts or loans or committing fraud or other crimes using the victim's personal information.

Figure 34. Javelin Categorization of Fraudulent Identity Transaction



Source: Javelin Strategy & Research, 2020

Deviation from FTC Reporting

When the report cites victims' average financial damages or resolution times in dollars or hours the entire amount of damages or losses is placed into every type of fraud the victims suffered. For example or a victim who reports that a total of $100 is obtained or both new accounts and other frauds category and existing card accounts the $100 is counted in both categories. This method of reporting costs by types of fraud will not change the overall total costs of fraud across all three categories but the average in dollars or time associated in the three types of fraud should not be summed because the result will be overlapping amounts.

Margin of Error

The ID fraud study estimates key fraud metrics or the current year using a base of consumers experiencing identity fraud in the past six years. Other behaviors are reported based on data from all identity fraud victims in the survey (i.e. fraud victims experiencing fraud up to six years ago) as well as total respondents where applicable.

For questions answered by all 5,000 respondents the maximum margin of sampling error is +/- 1.41 percentage points at the 95% confidence level. For questions answered by all identity fraud victims the maximum margin of sampling error is +/- 3.22 percentage points at the 95% confidence level.

javelinstrategy.com inquiry@javelinstrategy.com 925.225.9100