2019 Identity Fraud Study: Fraudsters Seek New Targets and Victims Bear the Brunt

06 March 2019 By: Kyle Marchini, Al Pascual

PERMISSIONS AND COPYRIGHT GUIDELINES

Javelin’s 2019 Identity Fraud Study provides comprehensive analysis of fraud trends in the context of a changing technological and regulatory environment in order to inform consumers, financial institutions, and businesses on the most effective means of fraud prevention, 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 sponsor, FIS, a global financial services technology provider, marquee sponsor Experian, a global information services company, and educational partner GIACT, a payment fraud mitigation company for making this report available to Javelin Advisory Services clients for their internal use only. The study is in its sixteenth consecutive year and is the nation’s longest-running study of identity fraud, with 79,000 consumers surveyed since 2003.

Only sponsors and partners of this year’s identity fraud study have sole rights to use of any graphics and data listed in the 2019 Identity Fraud Study exclusively for their marketing campaigns and any other public purpose.

Javelin retains the ownership of the survey, raw data, methodology and all other project deliverables. While Javelin may selectively grant other non-competing organizations selective rights to use the project’s findings in other public venues, we retain ultimate discretion over such decisions.

Javelin Advisory Services clients and other non-sponsors do not have immediate rights to cite any findings in their marketing campaigns, press releases, webinars, or any other external communications. Please inquire with your Javelin Relationship Manager about licensing rights to cite or otherwise reproduce data findings or graphs.

KEY HIGHLIGHTS OF THE STUDY
Snapshot: Fraud in 2018

Overall Fraud Rates Fall 15%

16.7 million  vs  14.4 million
2017 victims  vs  2018 victims

Total fraud incidence rates fell to 5.66% of consumers

More victims are personally paying out of pocket for fraud

23% of fraud victims had unreimbursed personal expenses in 2018
Nearly 3x as many as 2016

This overall decline is led by a decline in card fraud

This shift is largely the result of new fraudster focus on schemes, like new account fraud
OVERVIEW

2018 was a year of mixed success for consumers. After three years of successive increases in fraud rates, the overall fraud incidence rate fell notably from 2017, ultimately affecting 2 million fewer victims. Unfortunately, the resurgence of higher-impact fraud types such as new account fraud, account takeover, and misuse of non-card accounts casts a shadow over the progress made in fighting card fraud.

Thanks to the combined efforts of financial institutions, merchants, card networks, and other parties to the payments process, card fraud — the bread and butter of fraudsters since the rise of major payment card breaches — has become somewhat more difficult to perpetrate effectively. The EMV transition in particular has placed a significant roadblock in front of fraud rings that focused on counterfeit card fraud — one of the simplest fraud schemes to conduct at scale. Online, there is hope that initiatives such as 3-D Secure 2.0 and emerging features such as card controls will meet similar success.
As fraudsters’ primary targets have strengthened their defenses, the criminal economy is repurposing well-honed schemes to focus on new types of organizations. With comparatively limited experience with fighting fraud, these organizations have had little reason to invest in the tools, tactics, and personnel to effectively prevent, detect, and resolve fraud. For victims, this means a long, strenuous, and frequently expensive path to regaining control of their identity.

**Javelin’s Prevention, Detection & Resolution Model**

**Prevention**
- How it works:
  - Stops identity fraud at the source, preventing unauthorized access to and use of private data. If identity theft has occurred, these methods thwart the criminal’s use of private information to obtain funds.

**Detection**
- How it works:
  - Detection of fraudulent activity occurs through company monitoring systems, account monitoring, consumer alerts, reviewing credit reports, and other methods for identifying suspicious activity.

**Resolution**
- How it works:
  - After identity fraud has occurred, victims and the institutions holding their accounts use services and tools to restore their accounts, credit, and identity to its pre-fraud state.

**RECOMMENDATIONS**

**Secure document scanning with robust liveness detection.** Simply asking users to take a selfie with their identity document and even asking them to include a custom message is not enough to overcome today’s fraud threats.

**Move away from SMS one-time passwords.** With the continuing growth of mobile phone takeover, it is becoming increasingly evident that SMS OTPs pose little barrier to determined fraudsters. Responsive alerts through “tap to approve” push notifications or out-of-band biometrics requests are significantly more difficult for fraudsters to overcome. With even lower-end smartphone hardware continually improving and more and more consumers enrolling in mobile banking, the obstacles to these types of authentication systems are shrinking.

**Use multi-channel alerts to thwart account takeover.** Takeovers of mobile phone accounts to compromise one-time passwords also allow fraudsters to intercept alerts sent by SMS or phone call. In the event of suspicious or high-risk activity, victims should receive alerts through multiple channels, ideally channels that cannot be compromised as a unit.

**Embrace 3-D Secure 2.0.** By moving away from passwords and toward a more robust data-sharing framework, the updated 3DS protocol avoids the mistakes of its first iteration while meaningfully increasing the difficulty of card-not-present fraud. For merchants, this is a major opportunity to reduce exposure to chargeback losses, and for issuers it has the added benefit of increasing confidence in legitimate transactions, reducing the risk of false positive declines.

**Lenders need to move into stronger identity proofing quickly.** As loan origination moves online, lenders need to ensure that they have a well-rounded view of the applicant. Using identity verification tools like document scanning or digital identity alongside risk assessment like device reputation and behavioral biometrics/analytics, can meld
verification that the identity exists and is legitimate with assurance that the individual applying is not a fraudster and truly owns the identity being claimed.

**Nonbanks need to improve their authentication now.** Fraudsters are finding easy targets outside financial services. Rewards programs, merchants, mobile network operators, and other online accounts all have value for fraudsters but frequently lack any authentication method more robust than passwords, security questions, or SMS one-time passwords.

**Bolster authentication across channels to reduce cross-channel risk.** While mobile apps have access to a strong array of authentication options, other channels that are much more vulnerable to fraud tend to rely on outmoded options such as SMS one-time passwords for online logins and knowledge-based authentication within the call center. Moving toward using stronger authentication methods, such as out-of-band biometric pushes, can alleviate the risk of fraudsters’ gaining a foothold through one channel with weaker authentication methods.

**Banks should prepare for rising rates of familiar fraud.** Not only is familiar fraud devastating for victims, it is one of the most challenging fraud types for financial institutions to combat. With knowledge of the victim’s personal details and the potential for access to the victim’s personal devices, familiar fraud perpetrators can easily overcome basic identity verification challenges, like knowledge based authentication. Even tools like document scanning are only viable defenses if they also incorporate visual comparison of the applicant against the document with strong liveness detection.

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 2018 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 November 6-19, 2018. Final data was weighted by 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 from 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.
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 929 identity fraud victims the maximum margin of sampling error is +/- 3.22 percentage points at the 95% confidence level.
Contributing Organizations

The study was made possible in part by FIS, Experian, and GIACT. To preserve the project’s independence and objectivity, the sponsors of this project were not involved in the tabulation, analysis, or reporting of final results.