2018 Identity Fraud: Fraud Enters a New Era of Complexity

06 February 2018 By: Al Pascual, Kyle Marchini, Sarah Miller

PERMISSIONS AND COPYRIGHT GUIDELINES

Javelin’s 2018 Identity Fraud Report 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 Identity Guard, a leading provider of proactive identity theft protection services for consumers. This study is the nation’s longest-running study of identity fraud, with 74,000 respondents surveyed since 2003.

A thank you to our sponsor, Identity Guard, for making this report available to Javelin Advisory Services clients for their internal use only.

Only Sponsors of this year’s identity fraud study have sole rights to use of any graphics and data listed in the 2018 Identity Fraud report 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.

TABLE OF CONTENTS

Overview
Executive Summary
Key Findings
Recommendations
Organizations
Consumers
Key Metrics
Overall Fraud Trends
Existing-Account Fraud
Existing-Card Fraud
Existing-Non-Card Fraud
Account Takeover
New-Account Fraud
Prevention
Growing Complexity of Fraud
Data Breaches and Fraud
Detection
Alert Usage
Resolution
Fraud Severity
Responsibility for ID Protection
First-Time and Multiple-Fraud Victims’ Responses
Appendix
Methodology
Glossary

TABLE OF FIGURES

Figure 1: Javelin’s Prevention, Detection & Resolution® Model
Figure 2: Identity Fraud Overall Metrics by Survey Year
Figure 3: Existing-Account Fraud Metrics (2013–2017)
Figure 4: Existing-Card Fraud Metrics (2013-2017)
Figure 5: Existing-Non-Card Fraud Metrics (2013–2016)
Figure 6: Account Takeover Metrics (2013–2016)
Figure 7: New-Account Fraud Metrics (2013–2016)
Figure 8: Fraud Incidence Rate and Dollar Amount of Losses, 2011–2017
Figure 9: Existing-Account Fraud Incidence Rate and Dollar Amount of Losses, 2011–2017
Figure 10: Existing-Account Fraud Incidence Rate and Dollar Amount of Losses, 2011–2017
Figure 11: Consumers Who Had a Card Misused for POS and CNP Transactions, by Year
Figure 12: Existing Non-Card Account Fraud Rate and Amount of Losses, 2011–2017
Figure 13: Account Takeover Fraud Incidence Rate and Dollar Amount of Losses, 2011–2017
Figure 14: New-Account Fraud Incidence Rate and Dollar Amount of Losses, 2011–2017
Figure 15: Fraudulent New Accounts Opened Among NAF Victims, 2016–2017
Figure 16: Existing-Account Fraud Victims With Intermediary Accounts Opened, 2013–2017
Figure 17: Percentage of Account Takeover Victims Experiencing Cross-Account Takeover
Figure 18: Type of Information Compromised in a Data Breach, 2017
Figure 19: Fraud Incidence Among all Consumers and Notified Breach Victims (2011–2017)
Figure 20: Google News Search for “Data Breach,” January 2013–December 2017
Figure 21: Agreement that data breach notifications only help businesses (2016–2017)
Figure 22: Mean Days Until Fraud Was Detected, by Fraud Type (2016–2017)
Figure 23: Adoption of Alert Channels at Primary and Other Financial Institutions
Figure 24: Percentage of Consumers Who Have Modified Alerts Since Account Opening
Figure 25: Perceived Security of Online Banking, by Alert Engagement
Figure 26: Mean Number of Hours to Resolve Fraud
Figure 27: Perceived Fraud Severity, 2016–2017
Figure 28: Parties Considered Most Responsible for Protecting Consumers From Fraud
Figure 29: Resolution Steps Taken, First-Time and Multiple-Fraud Victims.
Figure 30: Financial Response to Fraud, First-Time and Multiple-Fraud Victim
Figure 31: ECF Victims Who Are Also Victims of Another Fraud Type in the Past 12 Months
Figure 32: Non-Card Accounts Affected by Fraud Among ENCF Victims, 2016-2017
Figure 33: Millions of Notified Breach and Fraud Victims (2012–2017)
Figure 34: Perceived Security of Mobile Banking, by Alert Engagement
Figure 35: Average Amount Consumers Lost to Fraud, by Year
Figure 36: Percentage of Victims Identifying Fraud as Having a Severe Impact on Their Life
Figure 37: Javelin Categorization of Fraudulent Identity Transactions

OVERVIEW

With all of the data and tools at their disposal and unprecedented levels of sophistication, criminals are engaging in complex identity fraud schemes that are leaving record numbers of victims in their wake. This degree of complexity, which can target a single victim but span multiple organizations, means that an organization can no longer reasonably expect to protect its customers through its efforts alone. In 2017, there were 16.7 million victims of identity fraud, a record high that followed a previous record the year before. None of the factors that contributed to this record and the other records set the past two years have subsided. As the disease of identity fraud reaches the level of an epidemic, prevention will require a new level of cooperation to eliminate the places that fraud has found to hide, fester, and
spread, while effective detection and resolution will become more important than ever before.

RECOMMENDATIONS

Consumers

Turn on two-factor authentication wherever possible. Enabling two-factor authentication on sites that have that capability, where a separate action must be taken beyond providing a username and password to access an account, can make it significantly more difficult for fraudsters to take over your accounts. For sites without two-factor authentication, use strong passwords or a password manager to secure accounts.

Secure your devices. With consumers increasingly relying on their digital devices to obtain goods and services, making purchases and sharing 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. 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.

Place a security freeze. If you are not planning to open new accounts in the near future, a freeze on your credit report can prevent anyone else from opening one in your name. This 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 prevents everyone except existing creditors and certain government agencies from accessing your credit report. Although costs vary per state, typically each bureau charges less than $20. Should you need to open an account requiring a credit check, the freeze can be lifted through the credit bureaus.

Sign up for account alerts everywhere. A variety of financial service providers, including depository institutions, 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.

Protect yourself from unauthorized online transactions. As EMV makes fraud at physical stores more challenging, fraudsters are now targeting 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 (e.g., Verified by Visa, SecureCode from Mastercard, etc.). These can help quickly detect and even prevent online fraud.

KEY HIGHLIGHTS OF THE STUDY

The Javelin Identity Fraud Report 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.

2018 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 1-16, 2017. 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, rounded up to the nearest whole unit, was used to calculate the median or mean value. For example: If the response selected for number of days to detection was one day to less than one week, the assigned value would be the midpoint of one day and seven days, inclusive, or four days. 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 accounts fraud instead of existing non-card accounts fraud. Javelin believes this change reflects a more accurate representation of debit card fraud, because much 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 for 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 for committing theft, fraud, or other crimes using the victim’s personal information.

**Deviations From FTC and 2003 Methodology and 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, for a victim who reports that a total of $100 is obtained for 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.

**Survey Questionnaire**

The set of questions and underlying methodology used for this report were identical to or highly similar to those in the 2017, 2016, 2015, 2014, 2013, 2012, 2011, 2010, 2009, 2008, 2007, 2006, 2005, 2004, and 2003 surveys. Some structural adjustments were made in 2011 to adapt CATI-based questions to web-based questions. All changes were made under the purview of experienced methodologists. Therefore, Javelin continues to provide longitudinal trends on various subjects, such as incidence rates and detection methods.

In addition, Javelin added a number of discrete new questions in 2012 to further explore the significance of past responses as well as to identify new trends around emerging technologies. In particular, Javelin sought to gain a better understanding of consumer behaviors regarding organizations contacted after fraud has occurred.
Margin of Error

The ID fraud report estimates key fraud metrics for 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 +/- 1.39 percentage points at the 95% confidence level. For questions answered by all 927 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 Identity Guard. To preserve the project's independence and objectivity, the sponsors of this project was not involved in the tabulation, analysis, or reporting of final results.