FROM APPLICATION TO TRANSACTION:

CARD FRAUD TRENDS, THREATS, AND TACTICS

April 2018

Sponsored by:

FIS

Independently produced by:

JAVELIN

TABLE OF CONTENTS

TABLE OF FIGURES

FOREWORD

This original report, sponsored by FIS, examines how payment card fraud is manifesting at the application stage and during transactions, and identifies the opportunities for financial institutions and other card issuers to preserve relationships with their customers by preventing, detecting, and resolving fraud.

This research report was independently produced by Javelin Strategy & Research. Javelin Strategy & Research maintains complete independence in its data collection, findings, and analysis.

OVERVIEW

Over the past several years, there's been an evolution in card fraud. With the advent of the EMV chip card standard, criminals are changing their digital habits, adapting with consumer trends and moving on from the point of sale (POS). As a result, card-not-present (CNP) fraud has accelerated and shows no signs of slowing down. Meanwhile, fraudsters are increasingly leaning into application fraud and with great success. The number of victims of new card account fraud is sharply rising — with crooks increasing their focus on private label credit and debit cards to find new profits. The onus is on FIs and issuers to simultaneously build higher walls, increase customer engagement, and better utilize digital technology to navigate the ever-shifting sands of payment card fraud.

EXECUTIVE SUMMARY

Key Findings

Application fraud, a $1.7 billion problem, is affecting an increasing number of victims. Criminals are increasingly opening fraudulent accounts in victims' names. Last year, the number of victims of fraudulent card accounts rose to 1.6 million from 0.9 million in 2016.

Transaction fraud losses are falling because of EMV and a shift in behavior. As more and more credit cards are meeting the EMV standard, criminals are focusing their attention on less lucrative debit and prepaid cards. In 2017, roughly 3.4 million people lost control of their prepaid cards — nearly three times as many as the previous year. The average amount per fraudulent transaction is declining. In the same period, debit card fraud victims rose from 5.2 million to 6.6 million. But the amount of cash those crooks are netting has been steadily falling over the past few years, from $9.7 billion in 2014 to $8.1 billion in 2017.

Traditional ID verification is broken and has given birth to new schemes such as synthetic identity and automated attacks. Fraudsters rely on the widespread industry practice of simply verifying personally identifiable information (PII) to determine the identity of an applicant. Continued reliance on traditional identity verification to prevent fraud during the digital application process has exposed FIs to the risk of rampant new account fraud as criminals take advantage of this oft-predictable process.

Breaches of all data, including PII and card information, increase risks. The precipitous rise in data breaches means that nearly all consumers' personal details are for sale on underground forums. Such marketplaces increase the risk that any customer can be affected by fraud.

Malware and social engineering are filling the gaps. This includes rudimentary types of devious software, such as keyloggers, and more advanced crime kits, which can include remote access Trojans and the ability to intercept ID data and circumvent identification and authentication controls. Criminals have also taken to conning customers and employees into releasing PII and granting access to accounts by phone, email, and even SMS texts.

Private label card origination growth has complicated managing fraud. For retailers, providing a positive and fast customer experience, especially at the point of sale, can contribute to less rigorous controls for preventing application and transaction fraud. For new private label cardholders, the ability to immediately gain access to a portion of their credit line has been a staple of retail POS card originations, but this practice opens the door to criminals looking to quickly monetize newly opened card accounts.

Intermediary account fraud is growing. Fraudsters are leveraging the breadth of PII at their disposal to open new accounts in the names of victims as a means by which to monetize existing accounts they have already compromised. The number of victims of these types of schemes has tripled in just the past year.

Fraud is shifting online as EMV becomes ubiquitous. Smart cards are making point-of-sale fraud increasingly difficult because those transactions are cryptographically guaranteed by the chip embedded in the plastic. In a search for profit, crooks are moving their craft

online, where it is more difficult for merchants and issuers to immediately prevent fraud.

Fraud resolution time exploded to 100 million hours in 2017. Between transaction and application fraud, the time victims spent resolving fraud more than doubled over the past two years, rising from 45 million hours in 2015 to 100 million in 2017.

Card application fraud creates very real victims out of consumers. Victims spend roughly 17 hours sorting through the details. That's almost three times as long as victims of existing credit card fraud take working through their issues. This results, unsurprisingly, in those customers' feeling frustrated and often quitting their banking relationships.

Recommendations

Empower customers with alerts, notifications, and cardholder controls. Give cardholders the ability to set limits on how a card can be used, including value thresholds and geographical boundaries, along with alerts that loop customers in on suspicious activity in real time, even prompting them to confirm or deny the legitimacy of pending transactions.

Create a holistic remediation process. FIs and issuers should take a holistic approach to managing the risk of card fraud in their portfolio and the subsequent negative effects on cardholders, which includes steps designed to prevent, detect, and resolve fraud to control losses and bolster loyalty.

Identify breaches early and adjust controls or reissue cards to get ahead of fraudsters. Being able to identify compromised cards as soon as possible is critical to preventing fraud from starting or escalating. This includes the use of common point-of-purchase analysis in which cards with known fraud become canaries in the coal mine for potential cases of account data compromise.

Issue EMV cards. Chip cards have proven to lower fraud at the point of sale as they effectively eliminate counterfeiting. They cryptographically prevent criminals from forging the plastic and using those fake cards at merchant locations.

Attack card-not-present fraud with technology. Implementing the recently enhanced 3D Secure protocol (3DS 2.0) facilitates the exchange of more useful data among the merchant, issuer, and network to authenticate the cardholder while controlling friction.

Use machine learning, document capture, behavior, and other identity proofing tools. A continued reliance on traditional identity verification to prevent fraud during the digital application process has exposed issuers to the risk of rampant new account fraud. FIs and issuers must use new tools to catch fraudsters, who are not only armed with all the data they need but are also now using that data and the knowledge that few additional controls are present to increase their effectiveness.

Adjust Day Two processes to catch application fraud sooner. Such processes are critical, as not all fraud will be caught during the application process. Strategically tightening controls on newly opened accounts and monitoring these new accounts for the first 90 days will help limit losses.

Give customers an easy, digital means of reporting fraud. Consumers expect to report fraud in the same way they'd digitally order a car from a ride-sharing service mobile app.

Issuers have to match the expectations companies outside of financial services have created for customers in every aspect of their relationship — including alerting an FI of a fraud event.

Keep customers in the loop on disputes. Providing regular updates on disputes via email or text so that cardholders can stay apprised of the status helps them quickly respond to requests for additional information.

INTRODUCTION

Often consumers' introduction to the world of financial crime is the shock of first hearing a line of credit has been opened in their name. The crime, which is the most popular form of identity fraud, can drive a wedge between cardholders and their issuers. Victims are likely to be placed on the defensive, questioned about any fraudulently opened account. Issuers may not be aware that criminals initially passed their identification process. The clash often results in outsized losses and high resolution times, alienating good cardholders from their issuers. For FIs and issuers — whose customers are pushing their cards to the bottom of wallets, abandoning accounts, and spending countless hours proclaiming their innocence — turning the tide of card fraud has never been more pressing.

CARD FRAUD TRENDS

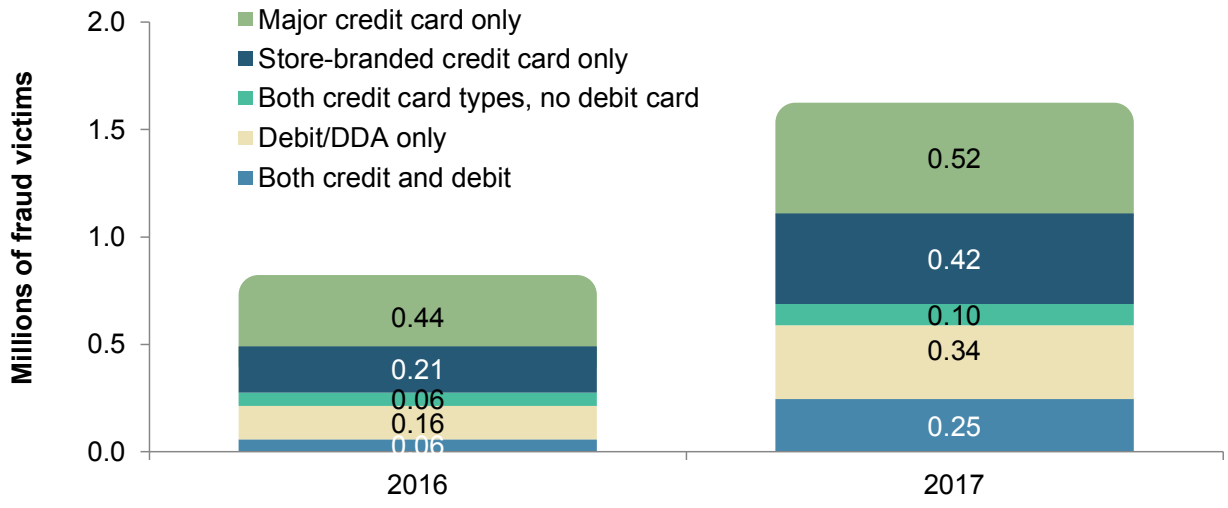
Application Fraud

Fraudsters are increasingly leaning into application fraud and with great success. The number of victims of fraudulent card accounts leaped from 0.9 million in 2016 to 1.6 million in 2017. But, despite their broader utility, application fraud involving general purpose credit cards did not grow at nearly the same rate as that on private label credit cards and debit cards (see Figure 1). For both it doubled over the course of a year.

Viewed in isolation, the growth of fraud in new card accounts may be misleading. Notice that the total amount lost to fraud involving these accounts actually declined to $1.7 billion in 2017 from $1.8 billion in 2016 (see Figure 2).

NAF Involving Store-Branded Credit Cards and Debit Cards Became Twice As Popular in 2017

Figure 1: Number of NAF Victims Having New Card Accounts Opened, by Type (2016-17)



Source: Javelin Strategy & Research, 2018

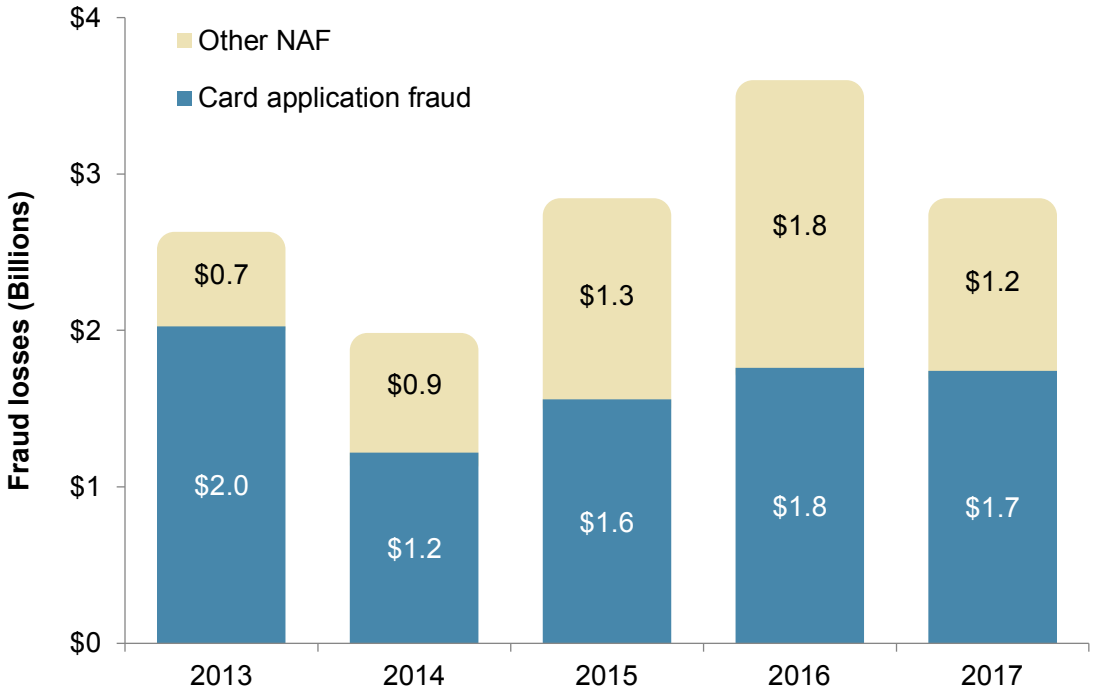
Taking a closer look, the changing nature of how and why criminals are opening and misusing new card accounts is in some ways positive news for FIs and issuers. For instance, new account fraud may be rising, but that does not correspond to higher losses. That means both that FIs and issuers are becoming more adept at stopping fraud and that upending what's left is becoming more challenging (*covered in more depth in the Fraud Drivers section*).

Transaction Fraud

The increasing focus on application fraud in some ways signals that criminals are shifting their attention away from transaction fraud. Most credit card plastic is now embedded with EMV chips, cryptographically assuring valid in-store payments. As a result, overall losses are declining as criminals move from credit cards, with their higher potential limits, to less lucrative prepaid and debit cards (see Figure

NAF Involving Store-Branded Credit Cards and Debit Cards Became Twice As Prevalent in 2017

Figure 2: New Account Fraud Losses, Card Application Fraud vs. Other (2013-17)



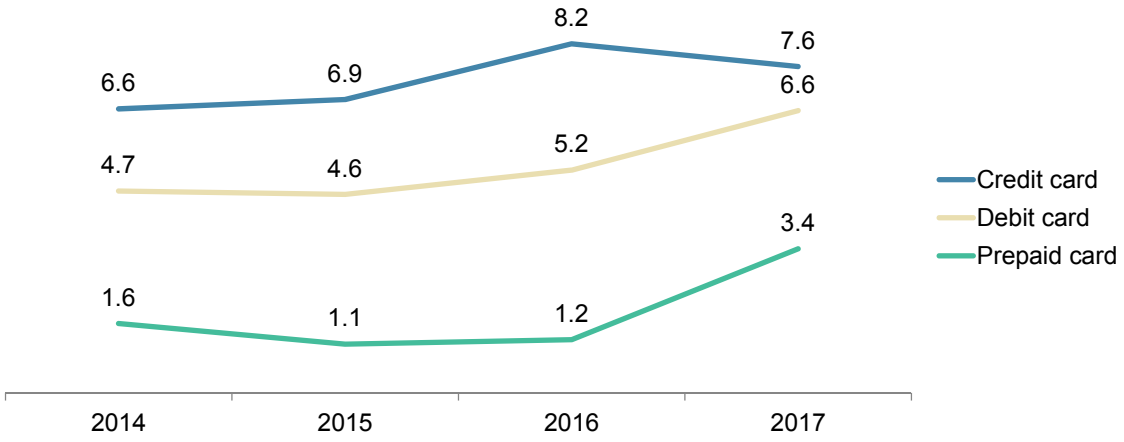
Source: Javelin Strategy & Research, 2018

3). This shift isn't haphazard — criminals are migrating to card types that are more likely to be magnetic stripe rather than EMV-enabled.[1]

Fraudsters are also standardizing processes and making their own risk-based decisions on how to commit payments fraud — optimizing their collective efforts. Criminals use test transactions to identify compromised cards with weak controls and to identify an operable range of transactions. The results of these practices are disseminated across the criminal underground through online forums — ensuring that only stolen cards that can effectively be misused are being sold and that the community has enough knowledge on how to use them successfully.

Credit Cards Remain the Top Transaction Fraud Target, but Debit and Prepaid Are on the Rise

Figure 3: Millions of Existing Card Fraud Victims, by Type of Card Misused (2014-17)



Source: Javelin Strategy & Research, 2018

[1] https://www.creditcards.com/credit-card-news/emv-chip-cards-one-year-later-consumer.php, accessed March 9, 2018.

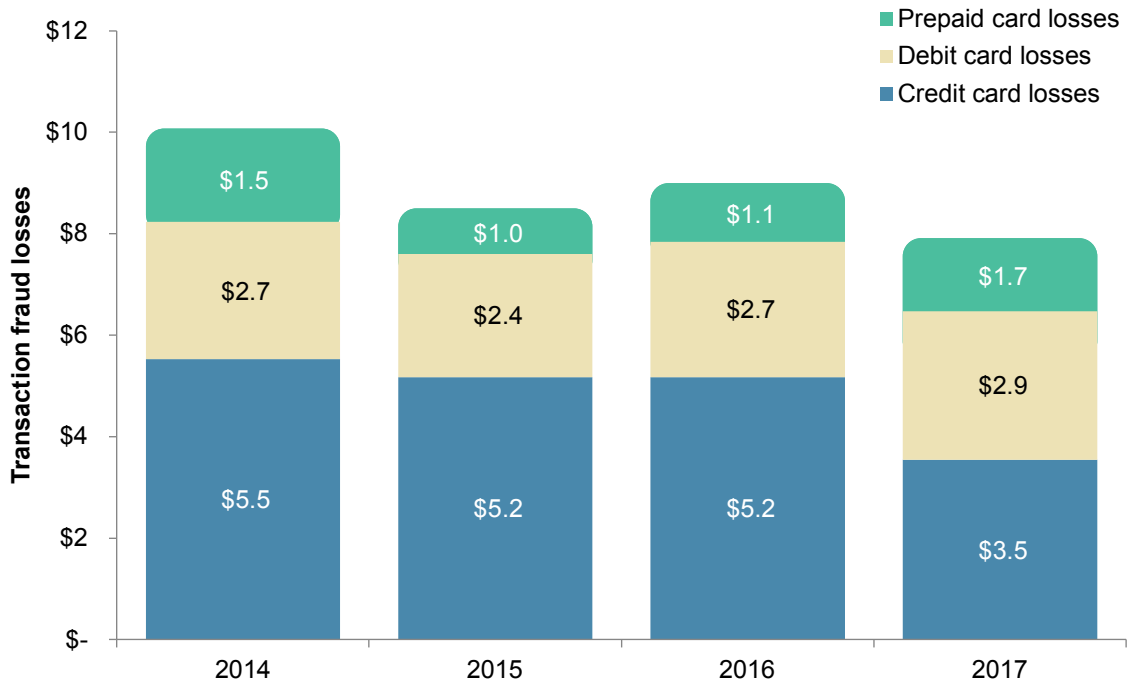
Despite the considerable growth in the number of victims where debit and prepaid cards were misused, the amount lost has not risen in kind. In fact, the fraud losses on existing credit card accounts have disproportionately declined. So while some of this decline may be the result of moving from more lucrative credit cards to lower-limit debit and prepaid cards, this change is also indicative of fraud transactions becoming smaller so as to avoid detection (see Figure 4).

Existing Card Fraud Is Shifting Channels

Online card fraud has been a significant challenge for several years in the U.S., having grown in tandem with overall online payment volume. So the rate of CNP fraud has accelerated and shows no signs of abating (see Figure 5). The mass adoption of EMV in the U.S. has driven fraudsters to gradually adjust their tactics, for example shifting to "buy online, pick up in store" as a bridge between their physical networks of runners and card fraud rings online.

Overall Transaction Fraud Losses Are on the Decline

Figure 4: Total Existing Card Fraud Losses in Billions, by Card Type (2014-17)

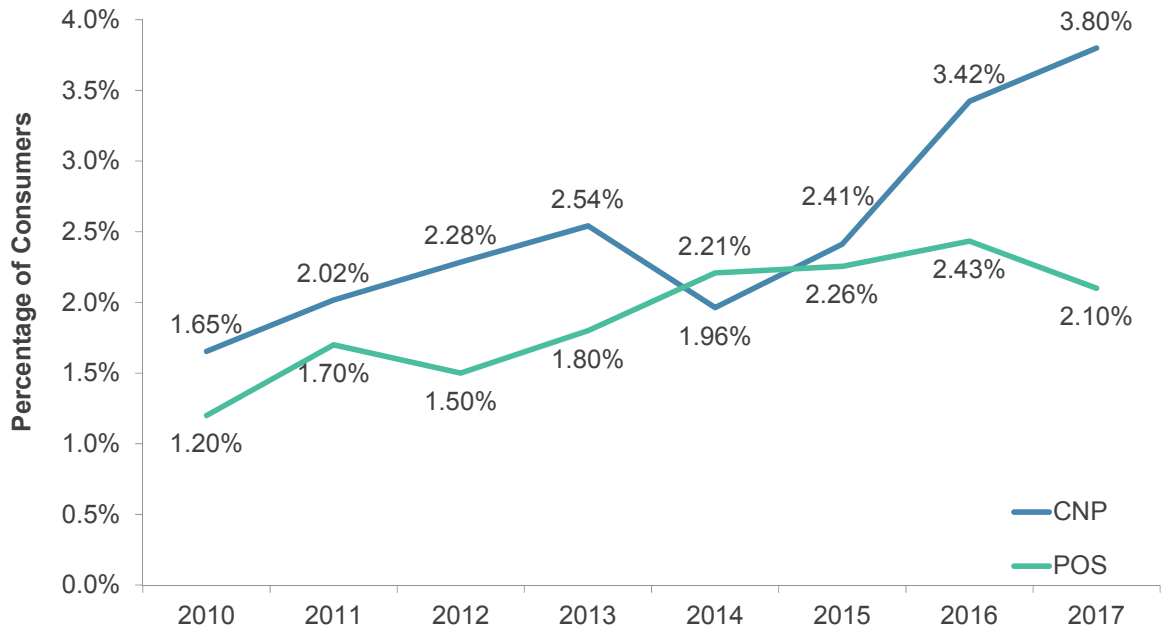


Source: Javelin Strategy & Research, 2018

The rate at which consumers are being affected by CNP fraud, having their cards misused for these transactions, will grow faster still as fraudsters evolve. These crooks often change targets, employing more sophisticated tactics designed to circumvent the controls of merchants and issuers, including the use of bots to complete transactions in volume. And they are shifting from physical goods merchants to digital goods ones that have less data to rely on and products that are more quickly and thoroughly monetized, such as virtual gift cards. Fortunately, POS card fraud is on the decline as EMV is taking hold despite the reluctance of some types of merchants to accept EMV (e.g., gas stations, restaurants, and hotels).

CNP Fraud Grows As POS Fraud Begins to Recede After EMV

Figure 5: Consumers Who Had a Card Misused for POS and CNP Transactions, by Year



Source: Javelin Strategy & Research, 2018

CARD FRAUD DRIVERS

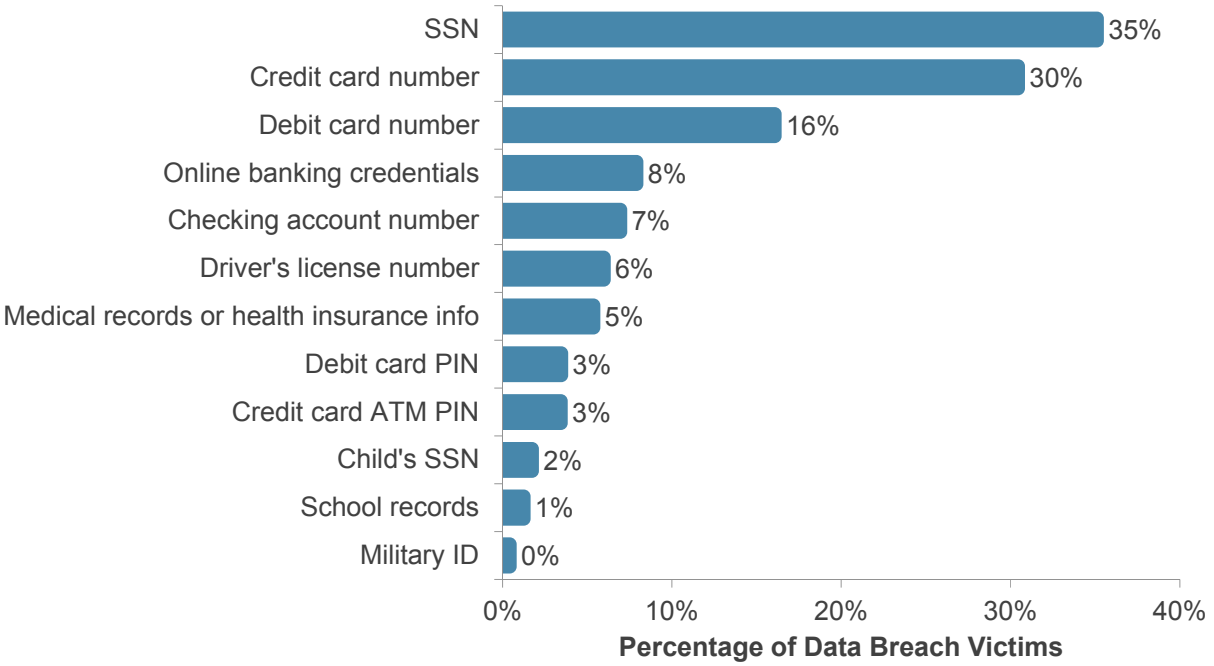
The drivers of fraud are both external and internal to the fraud management systems FIs and issuers employ. Outside the bank, criminals use malware, stolen data from breaches, and social engineering to compromise victims' PII. And when it comes to underground stores of consumers' details, there is little that isn't available to criminals. A variety of sources practically ensure a never-ending font of data is available where any type of data can be had and where every element of a consumer's identity information can be sold or traded without their knowledge.

Account Data Compromise

2017 was a monumental year for data breaches — the first one in which the compromise of Social Security numbers (SSNs) exceeded that of credit card numbers (see Figure 6, based on the proportion of notified breach victims). Plus, many SSNs compromised in breaches in years past are still valid, often having a shelf life as long as their legitimate owners. Breaches often yield several data elements, helping to complete the tapestry of identity elements required to commit more sophisticated identity crimes such as new credit card account fraud. And card breaches have far from disappeared as criminals must continue to source primary account numbers (PANs), expiry dates, and CVVs in order to be successful.

Social Security Numbers Were the Most Compromised Element of PII in 2017

Figure 6: Types of Personally Identifiable Information Compromised Among Notified Breach Victims



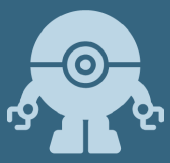
Source: Javelin Strategy & Research, 2018

Next, malware targeting consumers continues to evolve. Criminals are targeting consumers' mobile devices with increasingly sophisticated strains. This includes rudimentary types of devious software, such as keyloggers, and more advanced malware, which includes remote access Trojans and the ability to intercept and circumvent identification and authentication controls.

Unfortunately, all of this neglects that consumers are often the least secure guardians of their own PII. Social engineering remains a common means of attempting to secure PII and payment data. Some schemes trick victims into bypassing the fraud controls of their accounts when compromising a specific cardholder. Others play off fears to target a much broader audience, such as robocalls purporting to be from the IRS that threaten legal action, as a way to encourage consumers to call, share PII, or render payment information.

EXAMPLES OF ADVANCED MOBILE MALWARE

The Acecard Trojan, according to Kaspersky Labs, could bypass Google's Play Store to target Android users of almost 50 financial applications and services.[2]



GM Bot, which also targeted Android devices, was designed to superimpose a fraudulent message on top of legitimate mobile banking and payment applications. According to IBM X-Force Research, the malware was used to phish victims' online banking credentials, credit card information, and other PII.[3]

Source: Javelin Strategy & Research, 2018

[2] https://www.kaspersky.com/about/press-releases/2016_acecard-trojan-android-users-of-over-30-banking-and-payment-apps-at-risk, accessed March 8, 2018.

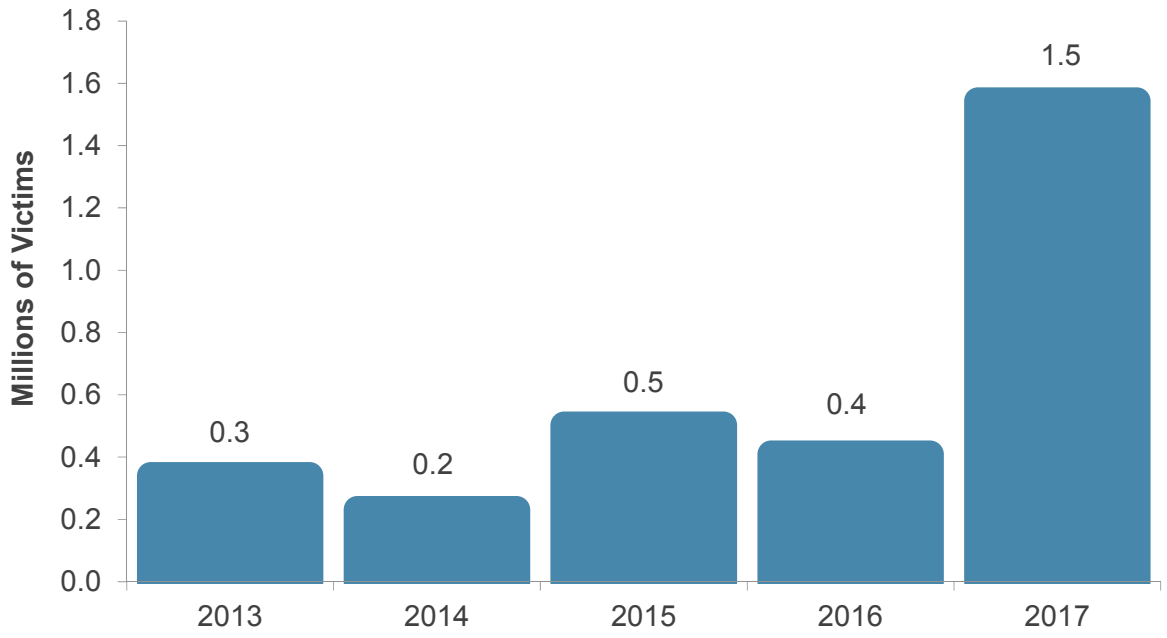
[3] https://securityintelligence.com/gm-bot-alive-upgraded-now-android-m/, accessed March 8, 2018.

Intermediary New Account Fraud

All these tactics describe a changing landscape in which the lines between traditional scams are blurred, complicating fraud detection. This is evidenced by the growth of "intermediary new account fraud," which has grown precipitously in the past year (see Figure 7). This crime involves fraudsters who intend to monetize a compromised existing account by opening one or more fraudulent accounts using the same victim's PII. These intermediary accounts can include services such as PayPal to more efficiently move cash out of a compromised account and new mobile phone accounts that can be employed to enroll compromised cards in mobile wallets.

The Number of Intermediary NAF Victims Tripled From 2016

Figure 7: Existing Account Fraud Victims With Intermediary Accounts Opened (2013-17)



Source: Javelin Strategy & Research, 2018

DISTINCT INDUSTRY CHALLENGES

Application Fraud

Inside an issuer, fraudsters rely on widespread industry practices and vulnerabilities inherent to the processes an institution relies on. A continued reliance on traditional identity verification to prevent fraud during the digital application process has exposed FIs to the risk of rampant new account fraud.

Criminals are armed with all the data they need and know that few controls exist to prevent them from increasing their effectiveness. They use a range of tactics:

Synthetic identities, digital mashups of identity information, include a combination of elements of PII. They can include data belonging to children and even fictitious people. These equivalents of Frankenstein's monster can help fraudsters evade detection by traditional identity verification controls and even subvert the process (e.g., credit bureau data, knowledge-based authentication (KBA), etc.). A synthetic identity can also be legitimized — think added as an authorized user on multiple aged accounts — and even form the basis for KBA questions later used to challenge the fraudster in subsequent application fraud attempts.

Automated attacks have become a viable method for completing application fraud when the issuer relies strictly on the verification of PII. Fraudsters can develop scripts for different institutions, based on the template of their applications, to automatically fill out various fields with the appropriate type of PII. This, in turn, allows fraudsters to increase the frequency with which they can submit applications.

Source: Javelin Strategy & Research, 2018

Private Label Complications

This is all complicated by the growth of private label card origination. Managing fraud on both new and existing accounts can be far more difficult than just accounting for general purpose cards. For retailers, providing a positive and fast customer experience, especially at the point of sale, can contribute to less rigorous controls for preventing application and transaction fraud, even when the controls are managed by issuer partners.

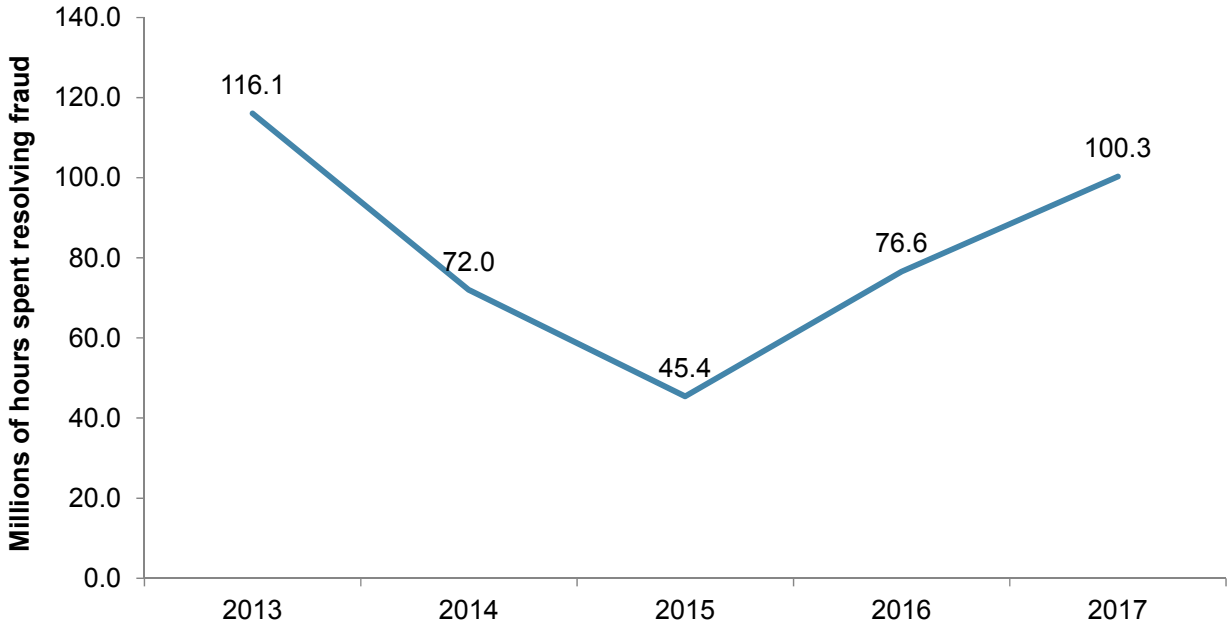
For new private label cardholders, the ability to immediately gain access to a portion of their credit line has been a staple of retail POS card originations. As private label card origination has migrated online, the bar for fraudsters has been lowered. In this new category, issuers must be concerned with trying to redirect a newly issued card to an address other than a fraud victim's true address. Criminals can now monetize freshly originated cards almost immediately when they are given real-time access to credit online.

THE EFFECT OF CARD FRAUD ON THE CONSUMER

Card fraud is often portrayed as a victimless crime. That's not true. Besides the losses incurred by issuers, consumers usually spend hours resolving card fraud. This ultimately undermines the relationship they have with issuers. Between transaction and application fraud, the time victims spent resolving fraud more than doubled over the past two years, rising from 45 million hours in 2015 to 100 million in 2017 (see Figure 8).

Victimized Consumers Spent 25% More Time Resolving the Effects of Card Fraud in 2017

Figure 8: Hours Spent Resolving Cases of Card Fraud, 2013-17

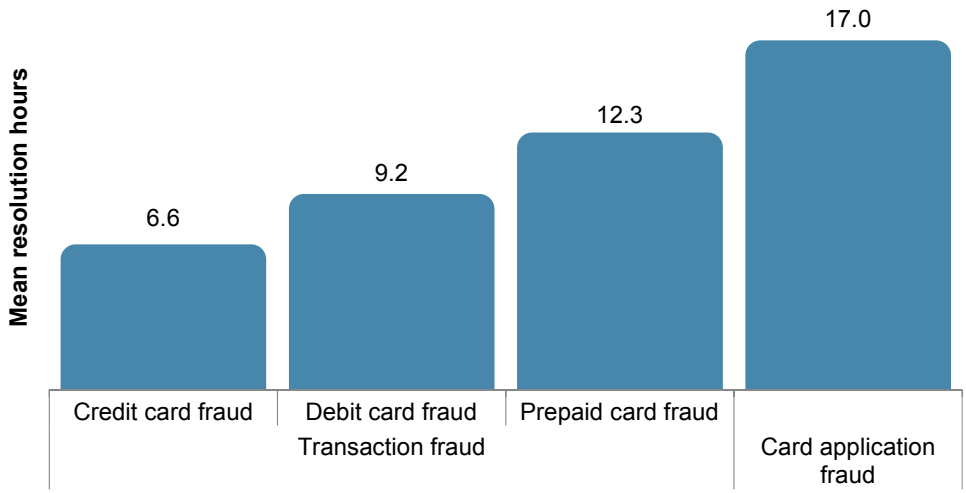


Source: Javelin Strategy & Research, 2018

Not all types of card fraud take an equal time to remediate. For victims of existing card fraud, there is a direct relationship between the liability protections they are afforded under Federal Reserve regulations E and Z (Reg E and Reg Z, in industry parlance) and the amount of time they spend resolving fraud. Provided the broadest of protections under Reg Z, credit card fraud victims spend the least time resolving fraud, followed by debit card victims whose liability is governed by Reg E. For prepaid cards, protections have only recently become more consumer-friendly, as consumers have begun to find protection under Reg E. But in cases in which a new card account is opened and no similar liability protections exist, victims spend almost three times as much time sorting through the details as do victims of existing credit card fraud (see Figure 9).

As Liability Protections Decline, the Time Consumers Spend Resolving Fraud Rises

Figure 9: Mean Resolution Time for Consumers, by Card Fraud Type



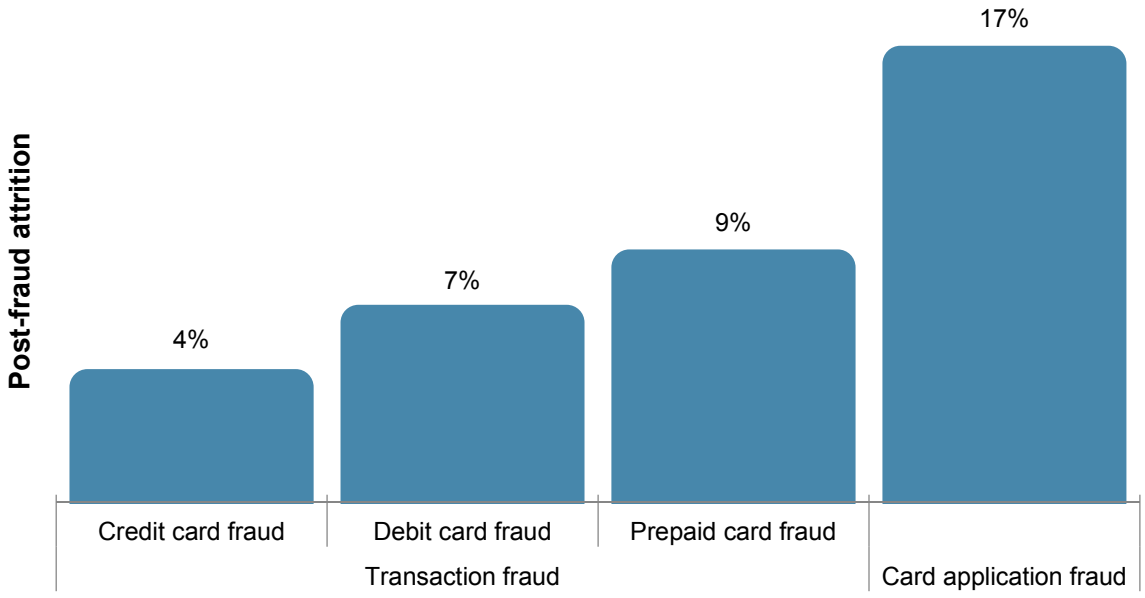
Source: Javelin Strategy & Research, 2018

Consequently, the decisions of some cardholders in the wake of fraud are unsurprising: They merely switch providers. For them, the time and energy they must invest in resolving fraud are just too much. Post-fraud attrition rates correlate with the amount of time victims spend in resolution.

Existing credit card fraud relationships are by far the least time-intensive and most sticky, and fraud involving new card accounts (where a link already existed) are most prone to attrition (see Figure 10). Also consider that the top driver for top-of-wallet choice is whether the customer is protected from fraud (see Appendix, Figure 11).

Existing Credit Card Relationships Are the Most Resistant to Post-Fraud Attrition

Figure 10: Percentage of Victims Who Switched Providers, by Card Fraud Type



Source: Javelin Strategy & Research, 2018

REMEDIATING CARD FRAUD IN 2018

Prevention

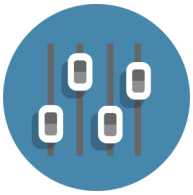
Fraudsters have become more sophisticated and their schemes more complex. Consequently, remediating fraud requires a holistic process that starts with avoiding it whenever possible. For that to happen, FIs and issuers must manage risk by matching fraud types with the most appropriate prevention strategies:

- **Existing card fraud:** Being able to identify compromised cards as soon as possible is critical to preventing fraud from starting or escalating. This includes the use of common point-of-purchase analysis in which cards with known fraud become canaries in the coal mine for potential cases of account data compromise.
- **POS card fraud:** The foremost step that issuers can take in specifically managing the risk of POS card fraud is EMV reissuance. The tactic prevents card counterfeiting, which is the leading danger for traditional magnetic stripe cards.
- **CNP card fraud:** Implementing the recently enhanced 3D Secure protocol (3DS 2.0) facilitates the exchange of more useful data among the merchant, issuer, and network. The process authenticates the cardholder while controlling for friction through risk-based authentication and more convenient forms of step-up authentication, such as biometrics.
- **Application fraud:** Evolving from identity verification to identity proofing in which the stages of the assessment process are updated and supplemented can mitigate the risk of application fraud from compromised PII, including synthetic identity, and moot the effectiveness of automated attacks. Adjusting Day Two processes is also critical as not all fraud will be caught during the application process. Strategically tightening controls on newly opened accounts and monitoring new accounts for the first 90 days will help limit losses. Similarly, any access to a credit line provided in advance of a customer's receiving the plastic should be limited, require additional layers of identity proofing, and ultimately be risk-based.

Detection

Meanwhile, detecting fraud as quickly as possible and minimizing its effects necessitate empowering cardholders to set thresholds and act as a second set of eyes for an issuer. The process can bolster a cardholder's perception of security and provide cover when transactions are initially declined for suspected fraud. This includes:

CUSTOMER-DEFINED CONTROLS



In which the cardholder sets limits on how a card can be used, including value thresholds, geographical boundaries, channel limitations, etc.

TWO-WAY ALERTS

Leveraging two-way alerts that prompt the cardholder to confirm or deny the legitimacy of pending transactions.

Resolution

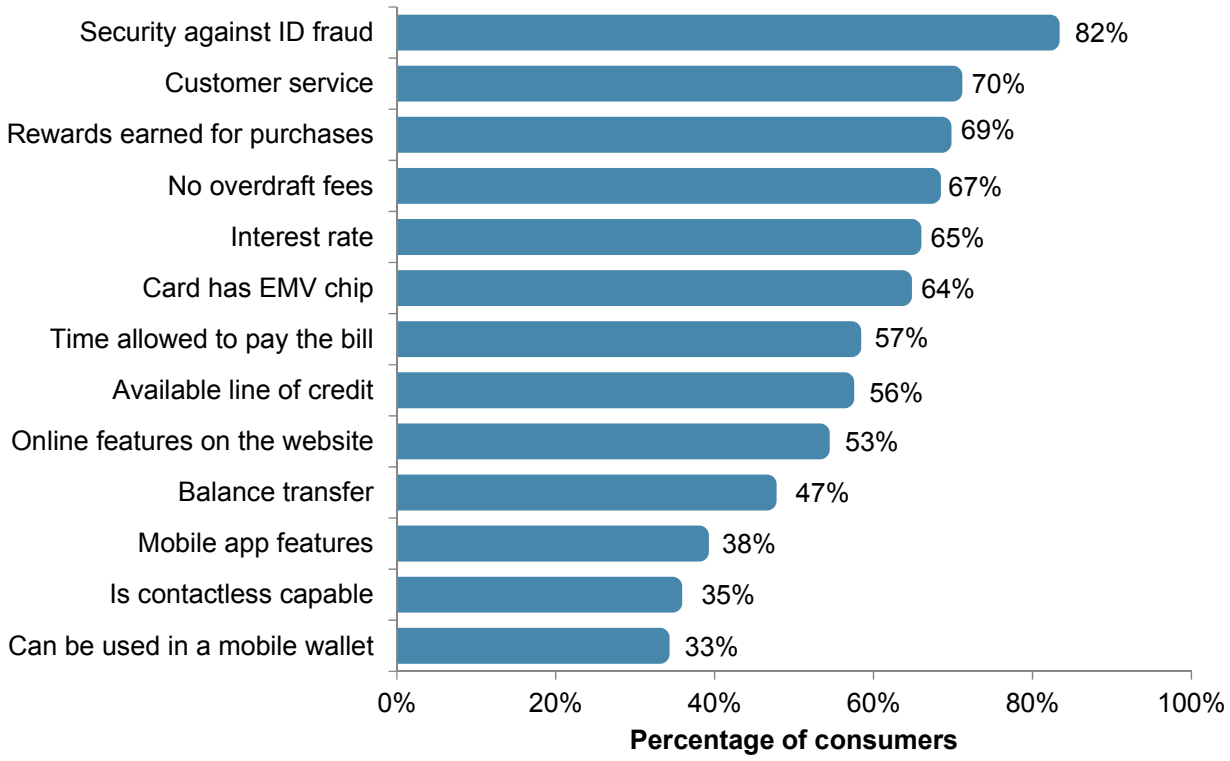
Finally, resolving fraud means FIs and issuers must leverage digital channels to increase convenience for customers and streamline the transaction dispute process as part of the transaction history. In doing so, the amount of friction imposed on the customer is lessened and, most important, the time customers spend resolving fraud is minimized. This capability may also manifest inside a security center in online banking or the mobile banking app.

Recognizing that this capability can increase costs as FIs and issuers are confronted with more claims, there are steps that can mitigate this potential. For example, the process should prompt cardholders to first contact the merchant in cases of non-fraud as they are best equipped to resolve the dispute. In addition, a virtual line of communication should be established, whether by email, text or through a banking app, that informs the customer of the status of a claim. Both of these steps are likely to improve the resolution process for the cardholder and subsequently reduce costs for the FI or issuer.

APPENDIX

Protection From Fraud Is the Most Influential Top-of-Wallet Driver

Figure 11: Most Important Factors in Choosing a Payment Card, All Consumers



Source: Javelin Strategy & Research, 2018

METHODOLOGY

Consumer data in this survey is based on information collected in the following survey:

- A November 2017 survey of 5000 consumers. The maximum margin of sampling error is +/- 1.39 percentage points at the 95% confidence level for questions answered by all respondents. Margin of error is higher for questions answered by smaller segments of respondents.

ABOUT JAVELIN STRATEGY & RESEARCH

Javelin Strategy & Research, a Greenwich Associates LLC company, is a research-based consulting firm that advises its clients to make smarter business decisions in a digital financial world. Our analysts offer unbiased, actionable insights and unearth opportunities that help financial institutions, government entities, payment companies, merchants, and other technology providers.

Authors: Al Pascual, Senior Vice President, Research Director
Sean Sposito, Analyst, Cybersecurity

Contributors: Kyle Marchini, Senior Analyst, Fraud Management

Publication Date: April 2018

ABOUT FIS

FIS is a global leader in financial services technology, with a focus on retail and institutional banking, payments, asset and wealth management, risk and compliance, consulting and outsourcing solutions. Through the depth and breadth of our solutions portfolio, global capabilities and domain expertise, FIS serves more than 20,000 clients in over 130 countries. Headquartered in Jacksonville, Fla., FIS employs more than 55,000 people worldwide and holds leadership positions in payment processing, financial software and banking solutions. Providing software, services and outsourcing of the technology that empowers the financial world, FIS is a Fortune 500 company and is a member of Standard & Poor's 500® Index. For more information about FIS, visit www.fisglobal.com.