MITIGATING APPLICATION FRAUD FROM SYNTHETIC IDENTITIES

April 2016

Sponsored by: id:analytics®

Independently produced by: JAVELIN
FOREWORD

This whitepaper, sponsored by ID Analytics, explores the challenges that FIs and issuers face against a rising tide of application fraud and how the sharing of intelligence offers long-awaited hope in detecting the synthetic identities that make it possible. JAVELIN independently produced the whitepaper and maintains complete independence in its data collection, findings, and analysis.

OVERVIEW

The long-anticipated arrival of EMV in the U.S. is contributing to a change in the nature of fraud as criminals shift tactics and focus on digital applications. Armed with a wealth of data and knowing that financial institutions (FIs) and issuers are ill-prepared to manage the threat, fraudsters are making synthetic identities a weapon of choice.
EXECUTIVE SUMMARY

Key findings

**Fraudsters refocus on new-account fraud:** With EMV limiting opportunities for fraud at physical points of sale, fraud rings that previously specialized in counterfeit card fraud are shifting to alternative means of acquiring physical cards. New-account fraud is especially attractive because it allows fraudsters to control everything about the account and provides the opportunity to cultivate high credit limit cards to generate maximum payouts.

**Breaches of persistent identifiers fuel new-account fraud:** 2015 witnessed a plethora of breaches of persistent identifiers – data such as Social Security numbers that retains its value for the entire lifetime of the victim. Much of this data is directly applicable to new account opening and can even assist fraudsters in answering dynamic challenge questions.

**Conventional fraud-detection solutions are ineffective at detecting synthetic identities:** Data validation solutions are prone to errors due to duplicated or incorrectly entered entries, which make it easy for synthetic identities to hide within the noise. Digital channel-specific solutions can be effective at identifying bots and devices with negative histories but fail to efficiently flag fraud executed from a clean device by an individual with no history at the institution.

**Consortium data can fill existing gaps:** Shared data on applicant identifiers and any resulting fraud within a consortium of financial institutions can fill gaps that exist in current fraud mitigation solutions. Not only can this intelligence assist with flagging synthetic identities, it can also provide advance warning of bust-out schemes as identifiers associated with a bust-out at one issuer are likely to be associated with similar risk at others.
Recommendations

Prepare for fraud to migrate from existing accounts to new-account applications:
With fraudsters already making strides in new-account fraud, issuers who wait to respond until they begin seeing charge-offs will be off guard. New-account fraud is one of the most costly fraud types because fraudsters can cultivate high-value accounts – acting like ideal customers until they leave issuers with massive losses.

Leverage community intelligence: Joining a consortium of financial institutions to take advantage of shared data on identifiers helps both screen new applications and monitor existing accounts. Because community data fills gaps in existing fraud mitigation solutions, it can provide significant fraud mitigation advantages when screening for synthetic identities.
FRAUD TRENDS AND DRIVERS

With the U.S. transition to EMV well underway, fraudsters are preparing alongside merchants and financial institutions. As EMV becomes ubiquitous both in cardholder wallets and at merchant terminals, counterfeit card fraud—the traditional first line of attack for fraud rings specializing in physical points-of-sale—becomes less attractive. These organizations have two alternatives—find some way to target the dwindling magnetic stripe holdouts or obtain “legitimate” cards.

In a short time, these holdouts will become much harder to identify. By 2019, magnetic stripe cards will constitute only 14% of the U.S. consumer credit card market and a mere 6% of the U.S. consumer debit card market (See Figure 1). This is undoubtedly good news for merchants, consumers, and financial institutions: By 2019, after a breach, fraudsters will be able to make counterfeit cards from at best roughly 1 in 20 debit cards and 1 in 6 credit cards.

By 2019, EMV Will Reach Near-Ubiquity for U.S. Credit and Debit Cards

Figure 1: Forecast EMV Saturation for U.S. Consumer Credit and Debit Cards (2015-2019)

WHAT IS A SYNTHETIC IDENTITY?

Identities used to fraudulently open new accounts can generally be divided into three categories:

- Stolen identities/true identities are composed of the complete/accurate core personally identifiable information (PII) of an individual, including name, SSN, and DOB.
- A synthetic identity does not imitate a true identity. Instead, it includes a name, SSN, and DOB where the SSN is not clearly associated with a known individual.
- A hybrid identity/manipulated identity comprises core PII in which the name, SSN, and DOB do not match but the SSN belongs to a known individual.

Because the data points used in fabricated identities (synthetic or hybrid) may either be individually valid or new to the system (and consequently difficult to flag as invalid), it is particularly difficult for financial institutions to identify them as falsified. Moreover, since no single fraud victim can step forward to claim such an identity, fraudsters are better able to use these patchwork identities as a foundation for a valuable web of networked accounts.
While card fraud is expected to transition to a greater emphasis on card-not-present transactions, this will largely be driven by organizations that already specialize in CNP fraud, since this fraud type requires very different skill sets and organizational structures than POS fraud. POS fraud works best with geographically centralized organizations built around networks of runners utilizing knowledge of vulnerable local merchants and local fences. This knowledge includes which merchants have upgraded their POS terminals, which have the most favorable return policies, and even what are typical merchant shift changes to avoid repeatedly meeting the same clerks.

Card-not-present fraud requires a geographically diverse set of shipping points to avoid having targeted merchants see clusters of fraudulent purchases associated with the same shipping addresses. This is typically facilitated by re-shippers – intermediaries that establish rotating networks of drop points for fraud rings to use in masking their locations. Additionally, successful CNP fraud requires knowledge of vulnerable merchant sites coupled with the technical skill to avoid leaving obvious trails from unmasked IP addresses and other device identifiers.

For POS fraud rings with established networks and infrastructure, it is more straightforward to shift to a new means of acquiring cards than to shift to a new means of acquiring goods. New-account fraud has a number of advantages in this respect. New cards are viewed as legitimate by the issuer, so EMV provides no barriers to their use in POS transactions. Moreover, by controlling the contact information provided to the issuer, fraudsters are able to circumvent some anti-fraud measures by contacting issuers to direct them to override security-related card declines. This allows fraud rings to gain substantially higher payouts from each card, despite a smaller number of cards being in their possession.

---

For fraudsters with longer schemes in mind, a new card can be cultivated with near-perfect behavior of regular purchases and repayment, enabling them to raise the credit limit and maximize the payout. This can be especially lucrative when spread across an array of accounts. Since all of the credit cards associated with an identity feed back into the same credit report, nearly all of the credit limits linked to the identity will be able to be raised at approximately the same time, multiplying the return for the fraudster and the losses for the issuers.

**New-Account Fraud Incidence More than Doubles from 2014**

Figure 2: New-Account Fraud Victims and Losses (2013-2015)

All of this is consistent with international experience. Following their EMV transitions, both the United Kingdom and Canada witnessed substantial spikes in both fraudulent card applications and account takeovers as fraud rings shifted to their next-best methodology. Unfortunately, the U.S. is likely to be in a far worse state.

When the UK converted to EMV in 2005, digital account application was still nascent. In most cases, applying for a new account was accomplished through a visit to a local branch. This imposed meaningful restrictions on fraudsters, who risked discovery from repeated visits to the same branches and who had to support their applications with falsified documents.

---

From the perspective of fraud mitigation, this was a far better situation than the contemporary U.S. market, where most credit card applications are conducted online. While digital applications undoubtedly improve customer experience and ease in account opening, they increase the complexity of fraud mitigation. Not only do online applications offer fraudsters greater anonymity, they can also be completed much more quickly and in greater volume as fraudsters immediately take identities from declined applications to the next target issuer, moving from site to site until they receive a positive response.

Unfortunately, the transition to new-account fraud has already begun. In 2015, the number of individuals victimized by new-account fraud more than doubled from 2014, rising from 0.7 million to 1.5 million (See Figure 2). This is low relative to previous years, so consumers and financial institutions should not start to panic, but the resurgence of NAF means that FIs cannot afford to wait to bolster defenses around account initiation.

---

Data Breaches and NAF

The push for POS fraud rings to move to new-account fraud has been supported by breaches of persistent identifiers key to the account application process. In 2015, 7 million individuals reported having their Social Security numbers breached within the prior 12 months, 63% more than in 2014 (see Figure 3). Since SSNs maintain their value for the entire life of the associated individual, these represent lasting vulnerabilities.

Direct identifiers such as Social Security numbers have straightforward application in the perpetration of fraud, but even data points such as medical or school records can provide fraudsters with an array of usable information. Health records can contain records of current and previous residences, schools, and relatives – all frequent sources for security questions.

7 Million Individuals Received Notifications of Breached SSNs in 2015, Including 1.2 Million Children

Figure 3: Millions of Consumers Notified of Compromised Persistent Identifiers (2014-2015)
More worrisome are breaches of information on children. In 2015, 1.2 million individuals reported that the Social Security number of their child had been compromised in a breach within the past 12 months (See Figure 3). Many of these likely came from breaches at health insurance providers such as Anthem, which hold rich information on both children and adults. Others likely originated from breaches at state agencies such as the Georgia Department of Community Health and the Arizona Department of Child Safety.\(^4\)

November’s breaches at VTech compromised the name, gender, and date of birth of more than 6 million children.\(^5\) Less than a month later, a breach at Sanrio that compromised 3.3 million user accounts, likely including a significant, but unconfirmed, number of minors.\(^6\) Not only did the Sanrio breach compromise names and birth dates, password reset question/answer pairs were also leaked, providing richer information on the breach victims that is also likely to be useful in financial applications.

Fraud using the information of minors is especially pernicious for both victims and financial institutions. Because these individuals often have limited financial histories, little or no information on them exists with the major credit bureaus. This provides a “blank slate” for fraudsters to work with in applying for new accounts, since there can be no negative flags associated with the identities. While the financial institution may see these identities as a credit risk due to the empty history, they will slide through most security screenings without a major problem.

For victims, this type of fraud can establish major financial roadblocks. Minors are unlikely to discover the fraud until they attempt to apply for an account themselves, at which point the fraud is likely to have been well established in their credit history.


APPLICATION FRAUD MITIGATION VS. SYNTHETIC IDENTITY

Data Validation

Under the Patriot Act, financial institutions and card issuers are required to verify core identity elements through a Customer Identification Program (CIP). Typically this entails validating name, date of birth, Social Security number, and place of residence. Additionally, CIP may include checks of ancillary data such as employer or contact information.

Complicating the process, this information is rarely verified directly. Since it is not possible to check SSNs directly with the Social Security Administration, these checks are typically performed with credit bureaus or third-party data vendors who aggregate a number of sources to a more robust picture of the identity.

Due to a variety of factors, these data sources may have identifiers associated with multiple identities. Legal name changes may result in the same SSN’s being associated with multiple accounts if records are not appropriately merged. Also, entry errors such as transposition may result in different SSNs’ being associated with the same name. These factors become significantly more complicated when considering more frequently changing data points such as home addresses and phone numbers. This fuzziness allows manipulated identities to blend in effectively as each data point appears valid, despite linking to a number of different identities.

Additionally, data validation solutions cannot confirm that the individual providing the information is the true owner of that information due to the anonymous nature of the digital application process. With the glut of information available from data breaches, even if an institution is able to confidently confirm that all identifiers provided belong to a single individual, there is no guarantee that the person completing the application is that same individual.
Digital Channel-Specific Tools

In attempts to deal with the challenges of digital anonymity, financial institutions deploy tools that can leverage digital intelligence. One such tool is device recognition/reputation, which profiles the devices being used to initiate applications to recognize any suspicious indicators. While much of the effectiveness of this tool is tied to historical behavior data (e.g., did the user who always uses a Windows machine in New York just log in from a Linux machine in Indonesia?), device reputation also has the potential to identify that a device completing a new application has been used to complete several other applications that resulted in fraud.

Rather than focusing on the device, user behavior analytics – also known as UBA, or behaviometrics – profiles a user’s interaction with his or her device and the institution’s website or app. By observing commonalities such as typical sequences of pages visited, use of proxies, and mouse, keyboard, and touchscreen interaction, UBA solutions provide probabilistic scores pointing to whether the current user is the same individual who has previously accessed the account.

Much like device recognition, UBA is most useful when able to reference past behavior of a given accountholder. When this data is not available, some inferences can be made from the manner in which the applicant interacts with the application, e.g. manual data entry vs. copy/paste, tabbing vs. clicking, and speed of completion. These all provide a security advantage during the application process in determining whether the application is being completed by a real human being or a bot.

While both of these types of tools have promise in preventing account takeovers, they are severely limited in their ability to stop applications completed with manipulated or synthetic identities. Since these applicants are by definition new to the financial institution, there is no history of either device characteristics or accountholder behavior to draw from. Unless a UBA solution detects that the applicant is using a program to autofill data or a device recognition solution connects the device with previous suspicious activity, neither solution will identify the application as fraudulent.
USING THE CONSORTIUM MODEL

The consortium model solicits data from all participants related to the use of different data elements and related experiences (i.e., positive or negative). Whenever a FI sees an identifier on an application, whether the application is approved or not, the identifier is submitted to the network. All other members of the consortium can check data points on applications they are receiving against the network in near real-time.

This gives FIs and issuers greater assurance that core identity data elements provided as part of an application all belong to a unique individual. Additionally, institutions can learn whether the data elements’ combined use is associated with fraud or known good account activity.

This provides an additional layer of security against new-account fraud using both stolen and synthetic identities. Identifiers that link to a wide variety of identities or that are associated with a large number of applications over a short period of time are more likely to be tied to synthetic identities.

Monitoring and reporting on PII on an updated, long-term basis can be effective in managing for bust-out fraud facilitated with synthetic identities. Over the long term, criminals may undertake bust-out schemes involving the regular use and payment of a credit card account so as to increase the limit, after which the criminal uses all available credit and defaults on the card.

This provides a long-term benefit even for financial institutions where stolen or synthetic identities slip through the initial application process. Learning that other institutions are experiencing fraud related to particular identifiers can give other members of the network the opportunity to more closely monitor accounts associated with those identifiers for suspicious activity.
METHODOLOGY

The 2015 ID Fraud survey was conducted among 5,111 U.S. adults over age 18 on KnowledgePanel; this sample is representative of the U.S. census demographics distribution, recruited from the Knowledge Networks panel. Data collection took place from October 15 to November 2, 2015. Final data was weighted by Knowledge Networks, 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.
ABOUT JAVELIN

JAVELIN, a Greenwich Associates LLC company, provides strategic insights into customer transactions, increasing sustainable profits and creating efficiencies for financial institutions, government agencies, payments companies, merchants, and other technology providers. JAVELIN’s independent insights result from a uniquely rigorous three-dimensional research process that assesses customers, providers, and the transactions ecosystem.

Author: Al Pascual, Senior Vice President, Research Director and Head of Fraud & Security
Kyle Marchini, Research Specialist

Publication Date: April 2016

ABOUT ID ANALYTICS, LLC

ID Analytics is a leader in consumer risk management with patented analytics, proven expertise and real-time insight into consumer behavior. By combining proprietary data from the ID Network— one of the nation’s largest networks of cross-industry consumer behavioral data—with advanced science, ID Analytics provides in-depth visibility into identity risk and creditworthiness. Every day, many of the largest U.S. companies and critical government agencies rely on ID Analytics to make risk-based decisions that enhance revenue, reduce fraud, drive cost savings and protect consumers. ID Analytics is a wholly-owned subsidiary of LifeLock, Inc. Please visit us at www.idanalytics.com.

© 2016 GA Javelin LLC is a Greenwich Associates LLC company. All rights reserved. No portion of these materials may be copied, reproduced, distributed or transmitted, electronically or otherwise, to external parties or publicly without the permission of Greenwich Associates, LLC. GA Javelin may also have rights in certain other marks used in these materials.