Back to the Future: The Resurgence of New-Account Fraud

Effective Fraud Mitigation Solutions to Help Combat the Next Generation of New-Account Fraud

Fraud detection best practices contributed to a decline in the amount stolen by fraudsters and the total number of victims in 2014. But enhanced defenses against a favorite target – point of sale – will compel fraudsters to refocus on other opportunities, including new accounts.

Financial institutions are making progress in their efforts to mitigate fraud. Between 2012 and 2014, the total amount stolen by fraudsters dropped from $21 billion to $16 billion. And the number of victims decreased from 13.1 million in 2013 to 12.7 million in the following year.[1]

The slow but steady transition to EMV* card transactions is contributing to the decrease in total fraud losses and the number of victims. Credit and debit cards made more secure with chip, tokenization and encryption technology make it significantly more difficult for fraudsters to engage in point-of-sale (POS) tactics in particular.

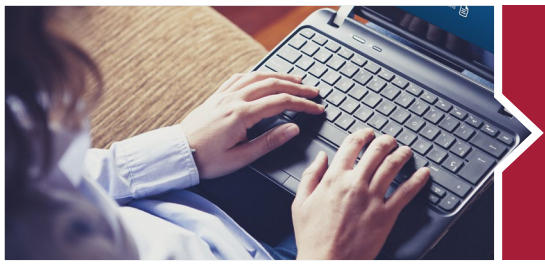
Higher-security cards make counterfeiting more difficult, if not impossible, noted Javelin Strategy & Research. Encrypted and tokenized information make data pulled from compromised terminals useless for future POS transactions.

**EMV (Eurocard, MasterCard and Visa) is a global standard for credit cards equipped with computer chips to authenticate transactions.*

New-Account Fraud to Climb

As organizations get better at fending off POS fraud tactics, fraudsters are expected to focus more of their activities on card-not-present fraud and another growing "revenue stream"— new-account fraud. Javelin estimated that new-account fraud will soar 44% between 2014 and 2018, rising from $5 billion in annual losses to a projected $8 billion.[2]

Obviously, financial institutions have implemented safeguards aimed at stifling attempts at new-account fraud. But because the take on successful new-account scams can be significantly greater than a typical credit or debit card scheme, fraudsters are expected to be persistent. New-account fraud can often go undetected for months unless the victim is regularly on the lookout for suspicious activity. And in the case of synthetic ID fraud, in which the fraudster creates a fake identity, the scam can go undetected for much longer.



Javelin estimated that new-account fraud will soar 44% between 2014 and 2018, rising from $5 billion in annual losses to a projected $8 billion.[2]

Synthetic ID fraud, often built on a real Social Security number (SSN), can be especially challenging to detect and prevent. New accounts are often created by people who don't have much of a recorded identity history. These can include coming-of-age consumers applying for their first credit card, or residents who have only just moved to the U.S. Making matters worse is that financial institutions may not have best-practice processes in place to verify an applicant's information.

Further, the fail-safes for many fraudulent activities are often not in place with synthetic ID fraud. Since real people won't see activity by an account created with mixed identity information – such as a real SSN, but a made up name or address, they're not going to raise any red flags. And when unusual activity does start to occur on a customer's account, a synthetic identity fraudster will promptly confirm that the suspicious activity is "legitimate" if contacted.

The facelessness of people who apply online for new accounts is expected to continue to make fraud detection even more challenging. With almost 88% of all Americans online,[3] the Internet remains their most popular banking method.[4] Banking online is growing in popularity and the use of mobile devices to manage accounts is rising. In 2014, 10% of the respondents said handheld devices were used most often to manage accounts, up from 8% the previous year.[5]

---

[1] Javelin Strategy & Research, *2015 Data Breach Fraud Impact Report*, June 2015

[2] Javelin Strategy & Research, 2015

[3] Internet World Stats, Usage and Population Statistics, June 2015 (www.internetworldstats.com/stats.htm)

[4] American Bankers Association, Press release: "ABA Survey: More Consumers Embracing Mobile Banking," Aug. 20, 2014

[5] American Bankers Association, Aug. 20, 2014

Identity Theft And New-Account Fraud

Credentials "with little apparent relationship to financial fraud will become important as a facilitator of new-account fraud," Javelin noted. For example, breaches of Social Security numbers affected 4.3 million consumers in 2013. The number of victims of an SSN breach who experience fraud in the same year is expected to grow 45% from 500,000 in 2014 to 710,000 in 2018.[6]

Unfortunately, SSNs and other identity information are readily available to criminals planning new account fraud schemes. Recent data breaches at universities, health care providers, government agencies, merchants and financial services companies are all high-value sources for SSNs.

The number of victims of an SSN breach who experience fraud in the same year is expected to grow 45% from 500,000 in 2014 to 710,000 in 2018.[6]

Increasingly, fraudsters are taking advantage of these data breaches to create synthetic identities using a combination of real and false information. In most cases, a synthetic identity or stolen SSN is presented like any other new identity to the credit-granting system. A typical example of a synthetic identity might include:

1. Social security numbers belonging to other people
2. Names fabricated by the fraudster
3. Dates of birth fabricated to match the appearance of the fraudster in case any "in-person" appearances are required
4. Addresses to receive mail fraudulently
5. Telephone numbers that are untraceable or stale by the time the fraud is realized

Once the identities are created, fraudsters typically nurture the identities and wait for them to mature. They may open accounts at different organizations, check their credit scores regularly and choose the perfect time to exploit the accounts to the maximum degree possible. In the aftermath, the financial-services organizations are generally left with a significant loss and no one to chase in their collection and recovery process.

[6] Javelin Strategy & Research, June 2015

Scenarios For Fighting Application Fraud

Much of the success that businesses have had in fending off fraudsters is a result of the increased sophistication of fraud detection technology. With robust fraud mitigation products from an integrated, real-time suite of solutions, organizations have the flexibility to better respond to shifting fraud tactics.

Here is how a suite of fraud mitigation products can help address two typical scenarios of new-account fraud:

Scenario I: Synthetic Identity Fraud

BUSINESS PROBLEM

A credit card issuer experiences fraud losses when fraudsters use fabricated account information, usually with a real SSN.

FRAUD SCENARIO

A card issuer offers credit cards via an online channel. Taking advantage of a potentially loose credit policy, fraudsters fabricate bogus identities. In most cases, the fraudsters concoct names and addresses, and give each identity a birth date within the 21 to 23 age range. Then they assign real SSNs to each fictitious applicant.

SOLUTION

To uncover the synthetic identity, screen each identity component.

The crucial first step in recognizing and combating synthetic identity fraud is to scrutinize the identity's components (such as name, address, Social Security number and telephone number).

Are they accurate? What is known from existing records about portions of the identity? The overall goal is to verify the existence of this identity.

Discrepancies in SSNs are frequently a tip-off to synthetic fraud. Robust identity fraud systems should be utilized to:

- Scan SSNs for high-risk factors — for example, has the SSN ever been issued by the Social Security Administration? Was it issued recently? Has the SSN been reported as deceased or misused?
- Does the SSN belong to a real person? Proprietary comparison algorithms can cross-check if the SSN matches the applicant's name, the name of another consumer or no names in the database. Systems can also determine if the SSN matches the birthday information of the applicants.

Similar scanning and cross-checking should also be done for other identity elements. Is the address real? Is there an actual home or business at that address? Do the applicant's name and other information correlate to a known person?

Scenario II: True-Name Identity Fraud

BUSINESS PROBLEM

Criminals use stolen identities to open new accounts via a lender's online or call center channel.

It is fairly easy for a criminal to obtain personal information (such as name, address, SSN and date of birth) to use in a fraudulent manner. As a result, identity theft continues to be a major white-collar crime in the U.S.

Identity theft can be defined as any act in which someone uses the personal information of another without that person's knowledge or consent. A common term for this type of identity theft, in which the fraudster poses as the actual consumer, is true-name fraud.

FRAUD SCENARIO

Relying on the anonymity of a lender's online services, a fraudster uses stolen personal information to apply for an account in the victim's name.

To detect attempts at true-name fraud, especially online, organizations need more than simple fraud tools that cross-check applicant-supplied information with various databases. Anti-fraud tools that just check the validity of the name, date of birth and address, for example, don't thwart criminals who have already obtained that information through some means of identity theft.

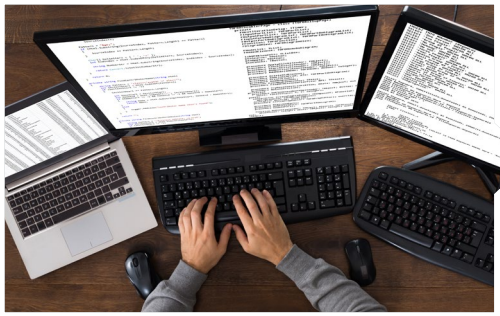
SOLUTION

Use a combination of authentication and modeling techniques.

Studies by Equifax have proved to show that predictive tools based on user behavior, velocity of activity, and known fraudulent behavior are an effective aid in spotting fraudulent applications in a real-time environment. Predictive modeling can demonstrably help reduce losses from true-name identity theft.

Optimum performance is achieved when the model draws upon a variety of data types, including:

- A business's own data identifying location, time and channel of past fraudulent incidents
- credit data for the consumer
- collections data for the consumer
- other proprietary information, such as fraud consortium data



Anti-fraud tools that just check the validity of the name, date of birth and address, for example, don't thwart criminals who have already obtained that information through some means of identity theft.

No One-Size-Fits-All Approach

Fraud is a difficult behavior to define — and even more difficult to predict. The fraudsters are constantly changing their methods, making patterns hard to establish. Therefore, predictive solutions must be continually updated with the latest data.

From a technology perspective, there is no cookie-cutter, one-size-fits-all approach to fighting fraud. Just as you might use several tools to repair a leaking faucet, several tools may need to work together for specific fraud detection and mitigation situations.

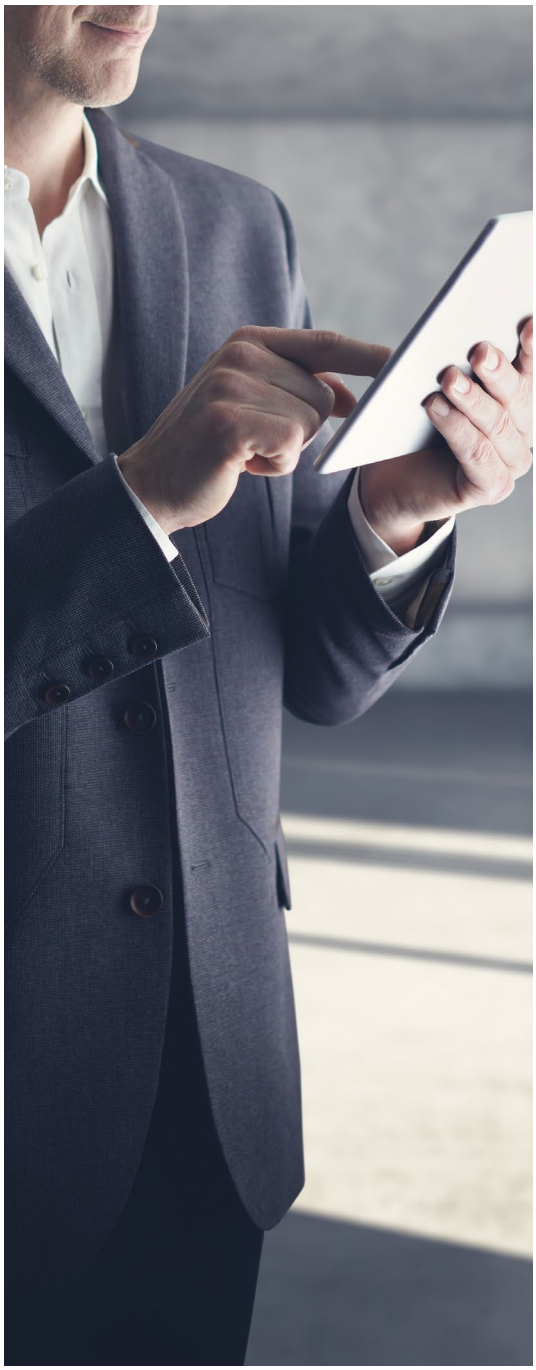
Advanced techniques often help identify true-name fraud at the source, at the time of application.

True-name fraud calls for a combination of strong defensive measures aimed at answering the key question: Is the applicant the person he or she claims to be?

Advanced techniques often help identify true-name fraud at the source, at the time of application. In the high-exposure online channel for credit applications, one proven technique is to ask the applicants several questions based on information that should only be known by the real person, such as the amount of a recent bill or credit charge. Moving toward a level of maximum security, the system should have the flexibility to support plenty of innovative, “out-of-wallet” questions from credit and non-credit sources, such as queries based on current or former employment.

Other tactics that organizations can use to prevent true-name identity fraud include:

- Performing transactional velocity checks to detect repeat attempts
- Using statistical models to provide a fraud index score as part of the overall assessment
- Leveraging non-public sources to minimize false positives



Six Challenges in Dealing with Fraud

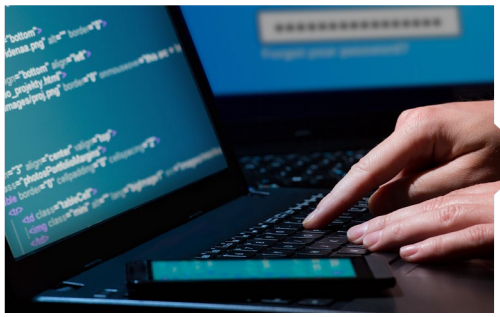
1. Fraud is hard to measure. Fraud has varying definitions, and even the definitions can be ambiguous. Consequently, many fraudulent transactions are written off as credit losses.
2. Fraud patterns are a dynamic, moving target. When organizations bolster their fraud defenses in one area, fraudsters seek new soft spots and shift their attacks to these less-protected areas. Different fraud types have notably different modus operandi and require different skill sets.[7] But fraudsters are not likely to close shop when presented with a new challenge. Instead, fraudsters constantly probe for the most vulnerable, least-defended areas and focus their efforts on these weak spots.
3. Fraud-mitigation efforts need to be dynamic, too. Organizations need to constantly scrutinize and upgrade their fraud defenses. Old methods may not need to be discarded — many of them still need to be in place, just modernized and expanded to keep up with fraudsters' ever-shifting tactics.
4. Fraud-containment efforts may collide with growth goals. Organizations understandably want to maximize new business opportunities. The dilemma is how to screen effectively for the likelihood of fraud without generating too many false positives — legitimate applicants who may be declined because they exhibit some traits often seen in fraudulent applications.
5. New customers and fraudsters both generally prefer the online channel. Look at the demographics of the customers you're trying to attract. More and more are likely to be younger professionals who rely heavily on the Internet. A new bank customer, for example, may be more familiar with the bank's website than its nearest brick-and-mortar bank. The trick is to grow online channels without taking on excessive fraud risk.
6. The scope of fraud activity is broad. Because there are so many aspects to fraud detection, prevention and resolution, and because they change so rapidly, fraud control managers face daunting challenges. There are no full-scale solutions that fit every lender's situation.

[7] Javelin Strategy & Research, June 2015

Summary

As fraudsters refocus their activities on new-account tactics, organizations will need to engage them with multiple layers of defenses that are nimble enough to address shifts in their strategies. With the right mix of fraud-mitigation tools, organizations can not only minimize losses, but also improve risk management and staff productivity.

Equifax offers effective solutions to help fight synthetic and true-name fraud, along with real-time detection of velocity and behavioral patterns indicative of suspicious activity.



As fraudsters refocus their activities on new-account tactics, organizations will need to engage them with multiple layers of defenses that are nimble enough to address shifts in their strategies.

Equifax's repository of industry-leading data helps provide deep insight around consumer identities. Our assets include credit, employment, income, demographic, telecommunications, utility, device ID and other differentiated data sources. We provide advanced analytics and technology innovations to improve fraud capture rates and effectively decrease false positives.

Our robust and reliable solutions help:

- Reduce fraud charge-offs and increase activation rates
- Improve the customer experience
- Improve fraud capture rates for high-risk transactions
- Reduce false positives

We welcome the opportunity to help you explore the best fraud mitigation approaches for your environment and level of risk.

CONTACT US TODAY

For more information:
1-877-262-5261
equifax.com/business/prevent-fraud