WHITE PAPER

Detecting and Preventing Banking Application Fraud

How analytics and artificial intelligence uncover the real challenge – synthetic identities

SAS THE POWER TO KNOW.

Contents

The illusive borrower

A man walks into a branch of the bank that issued his credit card. It's a good card, the record shows. Minor purchases and small cash advances have been swiftly and consistently repaid.

On this visit, the man requests the maximum cash advance permitted on his high-limit card. The teller obliges and hands the man several thousand dollars.

Before he has even reached the door of the lobby – poof – the man and the cash vanish into thin air. Apparently he was just a hologram all along.

Even a Hollywood special-effects expert would have a hard time pulling this off in the physical world, but in the digital world, it's easy. Create an identity, use it to steadily build history and trust – then make the big score and disappear. Poof.

The financial services industry is seeing a rise in this kind of disappearing act, for several reasons:

- More account openings – such as DDA accounts with overdraft protection, credit cards and other extensions of credit – are taking place through digital devices and the internet, which provide the access and anonymity fraudsters need.
- Data breaches expose large volumes of personal data for fraudsters to exploit. There is no real privacy for personal information anymore.
- The pressure to render real-time decisions on loan applications (or lose the business to a lender who will) cuts short the time available for thorough due diligence on a customer.

Granted, the trend toward online applications has both positive and negative aspects:

- On the downside, financial institutions lose the ability to verify applicants in person with the use of photo IDs such as drivers' licenses, passports and other paperwork. And one fraudster can generate a multitude of spurious credit applications, which would be impossible with traditional in-person, paper applications.
- On the other hand, the use of digital channels creates new information about device fingerprint, IP address, geolocation and more – data that can be folded into the analysis along with personal and credit bureau information to create a richer view of the customer (or the illusion).

These realities bring new urgency to fraud detection and prevention strategies. This is true not only for banks and credit card companies, but for other credit-granting organizations such as telcos, online retailers and auto finance organizations.

The role of specious identities in credit fraud

Application and online fraud, as well as bust-out fraud, often start with identity theft, alteration or the creation of synthetic identities. Synthetic identity theft is the fastest-growing type of ID fraud, surpassing traditional identity fraud in number of incidents.

According to Accenture, the fight has just begun:

> "Synthetic identity fraud is costing banks billions of dollars and countless hours as they chase down people who don't even exist. That is part of the reason why global card losses have been rising at an average annual rate of 18% in recent years, according to Accenture estimates.
>
> Synthetic identity theft alone may account for 5% of uncollected debt and up to 20% of credit losses, or $6 billion in 2016, according to some industry analysts. The problem is even more acute with store credit cards and auto loans."[1]

Gartner has a gloomier outlook, estimating that synthetic identity cases constitute 20 percent of credit charge-offs and 80 percent of credit fraud losses.[2] The US Federal Trade Commission estimated that synthetic identities account for nearly 85 percent of the 16 million ID thefts each year.[3]

It's definitely an issue worth addressing; synthetic identity fraud represented an estimated $800 million of losses in 2016, or an average of about $10,000 per account.[4]

Credit application fraud has several different flavors, but all involve the submission of false or manipulated information to influence credit decisions. Any credit-granting organization doing business on the internet faces the risk of application fraud.

Synthetic identities: The gold standard for application fraud

There are three key types of fraudulent identification: identity theft, identity manipulation and synthetic identities. Of these three types, synthetic identities tend to be the most challenging to identify, detect and prevent.

Synthetic identities are a combination of fabricated credentials – either totally created, assembled from various sources, or made by editing or changing breached data – where the implied identity is not associated with a real person. Hence, no one complains about a new unauthorized account, credit card or line of credit. That makes application fraud by synthetic identities particularly attractive to fraudsters.

Unlike identity theft or manipulation, where the core identity of a person is impersonated or manipulated by a fraudster, a synthetic identity is an artificial identity with no real person behind it. That makes synthetic IDs the first choice for initiating application fraud.

How fraudsters put substance to a synthetic identity

In the US, identity development begins with a Social Security number (SSN). Fraudsters obtain either actual numbers off the "dark web" or may create totally fake ones. When actual numbers are used, the criminals tend to prefer SSNs of children and deceased individuals – ideally, of deceased children. The criminal pairs the SSN with other personal and demographic information to create an identity.

[1] McIntyre, Alan; "The Battle Against Synthetic Identity Fraud Is Just Beginning," Forbes, Feb. 7, 2018 https://www.forbes.com/sites/alanmcintyre/2018/02/07/the-battle-against-synthetic-identity-fraud-is-just-beginning/#314d394c4ca0

[2] Groenfeldt, Tom, "Synthetic identity fraud in card not present transactions tops risk managers' concerns in 2016." Retrieved from https://www.miteksystems.com/blog/synthetic-identity-fraud-tops-risk-managers-concerns-2016

[3] Lanny Britnell, "The Changing Face of Identity Theft," US Federal Trade Commission, https://www.ftc.gov/sites/default/files/documents/public_comments/credit-report-freezes-534030-00033/534030-00033.pdf

[4] Pascual, Al; Marchini, Kyle; Miler, Sarah , "2017 Identity Fraud: Securing the Connected Life," Javelin Strategy and Research, Feb. 1, 2017. Retrieved from https://www.javelinstrategy.com/coverage-area/2017-identity-fraud

Once an identity is created, there are several ways to develop the appearance of a person through credit profiles or records. Three common methods are:

- **Applying for credit.** The fraudster uses the identity to apply for credit cards, phone service, etc. The merchant, financial institution or other entity submits the identity information to the credit bureaus. If the credit bureau has a file for that identity, it sends the creditor a score. If there is no comparable record, the credit bureau creates a file and records the inquiry. Whether the initial request is approved or declined, at least now a record exists for subsequent applications using that identity. It starts to look more real.
- **Adding an authorized user.** The fraudster adds a new identity as an authorized user on an existing and mature credit file – either another synthetic identity or a real person who may get kickbacks for colluding in allowing the fraudster to use their credit identity. By association, the newly authorized user adopts the credit score of the original account, then splits off to a separate credit file. The number and relationships of authorized users can be an indicator of this type of fraud.
- **Bringing a business entity in collusion.** This scheme, also known as a data furnisher approach, is likely to involve an organized fraud ring. Business entities (fake or real) create sham credit accounts for synthetic identities, then submit monthly records to the credit bureaus, making it appear that these accounts are being paid and represent real, credit-worthy people.

The underlying theme is the same: The fraudster exploits the services of the credit industry – banks, other creditors and credit bureaus – to build a credible identity to use to gain access to yet more credit.

Preventing application fraud starts with validating the identity of an individual using a digital device. Are they really who they say they are?

For financial institutions that really want to crack down on fraud, it's also about applying analytics and machine learning to spot out-of-the-norm behaviors, suspicious connections and the earliest signs of potential future fraud.

Verify identity at several layers of the digital application

Is the applicant a real person? Is he/she really the person represented in the application? Validating the identity of an individual using a digital device takes more than a standard credit check. It is about deep due diligence at multiple levels:

- **Identity verification** confirms that an applicant's details match historical records, such as from credit bureaus and other sources. This is the process of using external data to tie a user account to some sort of real-world identity.
- **Identity authentication** takes verification to the next level, ensuring that applicants are who they claim to be – typically by gathering information that cannot be easily forged or faked, such as a secret that would only be known to that person. Smart authentication relies on multiple data sources and matches the transaction's risk level.
- **Device verification** analyzes and compares device information to past experiences and the information provided by the person generating the application. Was this device used in the past, and was it associated with the same customer, account, etc.?

How to stop clever and ambitious fraudsters

Our "hologram" customer who disappeared with his cash advance followed the typical pattern of a bust-out scheme – open a line of credit for a fake identity, cultivate a good history for that account, then grab the big payoff.

The best analytical methods to detect bust-out schemes will vary depending on available data, the type of fraud and the phase of the endeavor – "make up," "pump up," or "run up and cash out." The detection strategy could include rules, anomaly detection, models, network analysis, machine learning and other statistical approaches. Multiple methods used together can very effectively find fraud while managing false positives.

Detection strategies for the make up stage

This is the phase where the fraudster manufactures identities and uses them to gain access to credit. To detect fraud at the point of application, organizations can gather clues from masses of internal and external data. Here are some effective approaches:

- **Monitor application data.** Building profiles of each data element in an application can help spot synthetic IDs and uncover the reuse of information across multiple identities or the reuse of the same laptops to create and manage multiple identities that are otherwise unrelated.
- **Assess past experience.** What is the creditor's past experience with applications that included the same data element, such as the same device ID, address or SSN? Were any declined? Were accounts closed for cause or fraud? Negative information may prompt further due diligence to understand the relationships between accounts and applicants.
- **Find "proof of life."** Many synthetic identities do not have records we would associate with a real person, such as driver's license, voter registration or property ownership. Lack of well-rounded identity details can be a strong red flag to a synthetic ID.
- **Analyze the network.** Network analysis plays a big role in understanding the connections (or lack of connections) among applicants, devices, open accounts and application data. For instance, does an account have authorized users who are not family members? Do multiple applications have the same credit file? Visualizations of these links can be very useful both in assessing applications and conducting investigations.

Detection for the pump up stage

During this period the fraudster cultivates the accounts by using credit lines in a normal fashion, making numerous small purchases and paying the account off each month, as any good credit customer would do. Over a number of months, the accounts develop a "normal" pattern and the appearance of good credit, which is used to request further credit line increases.

Machine learning for fraud detection

Scenarios learned from past experience are used as inputs for unsupervised or supervised machine learning, where the algorithm finds and learns from patterns in the data.

Unlike hypothesis-driven analysis, machine learning can uncover what you didn't know to look for. Machine learning has been shown to detect more fraud, even rare events that don't follow common patterns. It excels in finding the edge cases, people behaving out of the norm relative to their peers.

During this stage, the fraudster is building a good credit file, but there are rules and models that can identify suspicious or high-risk activity on these accounts. For example:

- Are payments from the same source (bank and account) being used to pay otherwise unrelated accounts?
- Is the same device being used to access and/or make payment on what appear to be unrelated accounts?
- Are credit lines fully used soon after account opening?
- Who is requesting credit line increases, and how often? Banks often offer increases, but in the case of fraud, generally the fraudster is making the request.
- Given the demographic data on the credit application, would the credit-holder be likely to purchase from the type of merchants where the account is being used?

Detection for the run up and cash out stage

Once the overall portfolio of accounts reaches a desired total credit limit, the fraudster (or organized fraud ring) then maxes out the cards and walks out the debt. Poof. In some cases, they will make a final payment with a counterfeit check and then max out the accounts again before the bank realizes the payment is worthless. The result: Even higher loss than the credit limit on the card.

It would be better to uncover the scheme before the run up and cash out stage, but there's still hope. Rules and models can detect late-breaking indicators, such as:

- Increased transaction frequency.
- Repeatedly maxing out a credit line and paying it off in full without carrying a balance.
- Payment on a card significantly before the payment due date.
- Payment by check when prior payments were made via online payment transfer.
- Network association with other accounts showing high-risk activity.

If a charge-off occurs, forensic analysis of the account can help you tune the rules and models for ever greater precision and support smart collection efforts. After all, there's not much point trying to collect from a synthetic identity.

Monitoring applications helps keep fraudsters from getting started, but data analysis really should continue across the life span of the account, including monetary and non-monetary transactions.

Elements of a solid application fraud solution

- A highly automated, **end-to-end** solution that spans the entire process from application submission to final disposition and reporting.
- **Data integration** from internal and external sources, such as device profiles, public records and portfolio data for existing, closed and previously declined accounts, customers and applications.
- **Advanced analytics** to extract insights from the available data, including rules, anomaly detection, models, network link analysis and machine learning.
- Approve/refer/decline decisions offered in **real time, near-real time** or batch modes, depending on rules violated or model score.
- A flexible and configurable user interface that presents all the information needed for decisions or investigations in **one intuitive portal** – with the ability to track and append the record as the process uncovers new information.
- User-defined reports and **data visualizations** in numerous formats, including graphs, charts, and network diagrams that uncover patterns.

Fraud detection analytics in action

Remember, in many cases bust-out fraud starts with a perpetrator opening numerous credit accounts with altered or synthetic identities. Monitoring the account throughout its existence – even toward the end – can detect suspicious activity early on and help prevent future loss.

And the losses can be staggering. Consider the 2017 case where a 63-year-old New Jersey man was charged with leading a fraud ring of individuals and sham companies that colluded with merchants getting kickbacks. One of the largest credit card fraud schemes charged by the US Department of Justice, this one involved more than 7,000 fictitious identities and 25,000 fraudulent credit cards, resulting in more than $200 million in losses.

Early detection analytics can dramatically improve the odds of discovering this type of activity. For example, SAS worked with an Asia Pacific bank to provide early detection of bust-out risk. Network analysis found:

- 60,000 contact phone numbers referencing immigration agents.
- 5,000 contact numbers referencing casinos.
- 2,500 phone numbers referencing the bank branch at which the application was made.
- 1,500 numbers referencing a meat processing plant.

These signs pointed to fraudsters flying below the radar with high-volume, low-value credit applications. With SAS, the bank found four times more application fraud, valued at $3 million a month, compared to its existing techniques. Furthermore, investigations were 2.5 times faster.

Conversely, analytics are also used to affirm legitimate applications that can then be fast-tracked to approval for a more positive customer experience, lower friction and fewer abandonments. With better application screening, good customers get expedited service, and bad ones are detected before they cause charge-offs and losses.

With hybrid analytics and machine learning, it's getting much tougher to make a living as a hologram customer.

Learn more

sas.com/fraud

To contact your local SAS office, please visit: sas.com/offices