APPLICATION FRAUD

Overcoming the Identity Challenge

Shirley Inscoe, Aité Group

Contents

Application Fraud:
Overcoming the Identity Challenge

By Shirley Inscoe, Senior Analyst Aité Group in partnership with GBG

Whether financial institutions (FIs) are processing requests for demand deposit accounts (DDAs), credit cards, or consumer loans, application fraud is a major challenge. Fraudsters easily commit application fraud by stealing another consumer’s identity, manipulating identity elements, or creating a synthetic identity out of thin air. It has even become very difficult to properly identify a consumer in a physical branch location due to technology innovations that enable the creation of almost-perfect counterfeit drivers’ licenses and other identity documents. Proving individuals are who they claim to be is harder today than ever before. With identity crimes increasing, FI executives need solutions that go beyond simple rules to enable them to keep false positive rates low while detecting the fraud that is increasingly pervasive. Solutions using machine learning and other complex analytics are effective in achieving these goals.

FI executives identify several pain points that lead to successful application fraud. By far, the biggest pain point is first-party fraud,[1] which 76% of executives cite as one of their top three challenges. Data breaches are the second-biggest problem. Much of the data breached can be used by fraudsters to impersonate real consumers or to extract data points to create a synthetic identity. Third highest among pain points is the social engineering that occurs in contact centers where fraudsters can successfully impersonate existing customers or open new accounts, committing application fraud.

[1] See Aite Group’s report *Application Fraud: Fighting an Uphill Battle*, December 2018.

Pain Points Leading to Application Fraud

Many pain points enable fraudsters to successfully commit application fraud. Here are the most common ones, ranked in order of severity by FI executives:

- First-party fraud (i.e., fraud committed by the person who owns the account) is extremely difficult to thwart, particularly if it is the first time the person has committed fraud. Organized fraud rings often recruit and incentivize people to perform certain tasks. In the case of application fraud, they may convince people to allow their personal information to be used to open new accounts or apply for a credit card. Various groups of people are targeted and approached by fraudsters—groups such as those who are young and naive, elderly people who may be easily misled, or people who have been in the country for a specific time period and are leaving shortly.
- Data breaches have occurred so frequently that people aren't as concerned as they used to be. That is unfortunate, because continuing data breaches refresh the data fraudsters gather about us all, and they are able to use this data to commit their crimes. There is no end in sight for these breaches, and many experts believe that a dedicated hacker will eventually gain access to any system.
- Social engineering in contact centers is a form of attack against an FI. These tactics are used by fraudsters to call repetitively until they can convince an agent that they are the real customer. In the case of application fraud, their job may be easier because they just need to convince the agent that they match the identity they are providing. This may be an identity they have created, or they can use data from data breaches, social media, and other sources to represent someone else. In one example, a fraudster called an FI's contact centers and opened over 50 DDAs using various identities.
- Scams often go hand in hand with elder abuse, but people of any age can fall for a scam. Elders are particularly vulnerable because they may be lonely, may be isolated, and may not have anyone who can advise them against falling for the scam in question. Elder abuse is prolific and is expected to grow as the population ages.
- Phishing attacks continue to flourish. According to the Anti-Phishing Working Group, in Q2 2018, 36% of phishing targeted payments and an additional

16% targeted financial institutions.[2] Phishing attacks have grown far more sophisticated both in their wording and in the methods used to conduct the attacks. In Q2 2018, about 35% of phishing attacks were hosted on websites that had HTTPS and SSL certificates (leading many to think the websites were secure and could be trusted). Most phishing attacks are sent to thousands of people, making even a low percentage of responses highly profitable.

- Identity theft and the use of manipulated or synthetic identities are challenges for FIs. Identity theft occurs when someone uses the identity of a consumer without their consent; the true owner of the identity is the victim. When fraudsters use synthetic identities, there is no victim of the crime because the identity does not exist in the real world. Fraudsters are nurturing synthetic or manufactured identities for many months or years, establishing credit bureau reports, obtaining mobile phones, and taking other steps to make such identities extremely difficult to detect.
- Malware has been a threat for almost as long as the internet has existed, and it has spread beyond computers to infect mobile devices as well. Many devices have malware, and while not all of it is malicious, FIs must guard against activity from infected machines.
- Authentication failures occur when a method used to authenticate consumers is defeated by fraudsters. For example, knowledge-based authentication (KBA) questions may be successfully answered by fraudsters based on data from data breaches, information posted on social media, or phishing attacks. Authentication gaps occur when fraudsters figure out a way around a fraud prevention or authentication process (e.g., a fraudster who doesn’t want his voice analyzed by contact center technology calls a branch and is transferred directly to an agent, avoiding the voice analysis performed on all incoming contact center calls).

[2] “Phishing Activity Trends Report: Second Quarter 2018,” Anti-Phishing Working Group, October 18, 2018, accessed November 22, 2018, http://docs.apwg.org/reports/apwg_trends_report_q2_2018.pdf.

Current Fraud Prevention Practices

FIs use a variety of processes and systems for fraud prevention and compliance purposes during the application process. Some of these systems may be queried during the process, while others are often run in batch and alert processing is handled the next business day.

FIs use many different types of solutions to understand who is opening new accounts and to prevent application fraud. About 75% of FIs use solutions that verify the identity with third-party databases and check with a consortium database to detect prior account abuse or fraudulent behavior. Roughly 60% of FIs surveyed also use KBA to determine that the person is who they claim to be and then also do a credit bureau query. Unfortunately, while some of these practices are widespread in the industry, the value from a third-party database or credit bureau query has been degraded due to all the data breaches and fraudsters' practices of nurturing synthetic identities until they are well-represented in both third-party databases and credit bureau files. Similarly, KBA questions can sometimes be more readily answered by fraudsters than the true individual, thanks to data breaches and all the personal details consumers post on social media websites.

FIs' satisfaction levels vary with the most commonly used fraud prevention solutions. Queries to consortium databases result in at least "somewhat satisfied" executives across the board. For credit bureau queries, verification of data to third-party databases, and dynamic KBA questions, there is some level of dissatisfaction among FIs. Some of this dissatisfaction stems from a lower reliability of the data than was available in the past. This is not the fault of solution providers but is instead due to data breaches, phishing attacks, and other methods fraudsters use to defeat these tools.

Another source of dissatisfaction with fraud solutions is the high rate of false positives often generated by some products. Adjustments to each system must be made to keep the number of valid alerts generated to a manageable level while not excluding alerts that indicate fraud. This balance is always the goal, but the correct balance is easier to achieve with some solutions than with others.

The majority of FIs (67%) have a target review rate between the 5-to-1 and 10-to-1 range. This means that they will work between five and 10 alerts that are false positives for every alert that represents actual fraud. Amazingly, 18%, or almost one in five, of FIs state that their target manual review rate is 31 to 1 or higher. Some systems produce such high false positives, perhaps these FIs have just resigned themselves to looking for the needles in the haystack. The primary danger of such high false positives becoming a way of life is that analysts may miss the fraudulent items because they find so few of them daily. Of course, these high rates also require more staff to review the alerts, resulting in poor operating efficiency.

New Technologies Can Help Solve the Application Fraud Dilemma

Many FIs have turned to implementing additional technology solutions to try to defeat fraudsters from successfully opening new accounts. Almost half (48%) do a verification on the opening deposit made to a new DDA. While only 11% indicate they are using a machine-learning engine, the use of this technology is expected to grow rapidly. FIs that are using machine learning are experiencing improved fraud detection as well as lowered rates of false positives. High false positive rates require excess manpower to process all of the alerts generated, inflating operating budgets.

Behavioral biometrics, used by 7% of FIs, is another relatively new technology that can help in identifying human versus nonhuman or bot behavior, as well as normal applicant behavior versus fraudster behavior during the application process. Other tools, such as IP geolocation comparisons, phone number verifications, one-time passwords, and fraud anomaly detection, are in use and expected to grow because they improve security without introducing friction into the process. These tools can be used to improve the customer experience while still adding an extra layer of security.

Delivery Channel Implications

FIs are opening more accounts than ever before through faceless delivery channels—online, mobile, and contact centers. While this is great for lowering operating costs, higher fraud rates are experienced in these channels than in traditional branch locations. This growth trend in digital channel volume is expected to continue, with the majority of growth in online and mobile channels. Consumers love their mobile devices, and with FIs using identity document verification and onboarding tools to help prefill data into an application with little manual keying, errors are reduced and security is enhanced all in one step. This is important in making the application process as efficient and pleasant for consumers as possible.

Organized criminal rings vary their attack methods over time. As a result, application fraud rates change in different delivery channels based on the methods and other factors (e.g., new capabilities rolled out for online or mobile channels). Over the course of the past two years, application fraud has increased in many FIs in all delivery channels to varying degrees. Over half of the FIs in the U.S. saw application fraud growth online, a third saw growth in branch-originated fraud, and 24% and 29% saw growth in mobile and contact center fraud, respectively.

Orchestrating Authentication

The key to containing application fraud as a result of identity crimes is to orchestrate authentication techniques until the FI is certain whether the applicant is who he or she claims to be. This doesn’t have to be onerous for the customer—in fact, it cannot be, or the good applicant will simply go somewhere else. Fortunately, FIs can use many tools to authenticate an individual with little or no friction. If an applicant has other relationships with the institution, it should be easier to ascertain whether he or she is the legitimate customer. Tools such as verifying a known device previously used by the customer, looking at patterns of activity in how the individual interacts with the device being used, and using biometrics stored on a device are all beneficial and almost transparent to the applicant. These tools can also be helpful with evaluating a new applicant the FI has not seen previously. For example, while behavioral analytics has not yet established a pattern of interaction with a device for an applicant, there are specific traits that can identify bots completing applications and identity fraudster versus normal applicant behavior in completing applications. Capturing data related to the device used to open a new account is an important step for future authentication measures to protect against potential account takeover fraud.

Each FI has a unique strategy to authenticate customers and ensure applicants are who they claim to be. Reliable authentication is the foundation of effective fraud prevention. As FIs employ a variety of solutions, they often use a waterfall approach with stepped-up authentication for high-risk transactions or a stepped-down approach for low-risk activities. Orchestration of authentication seeks to better analyze the customer’s usual behavior patterns as well as the context of the transaction. It does away with the one-size-fits-all approach and instead only inserts the friction of stepped-up authentication when necessary, (i.e., when the analytics flag that the context of the transaction is unusual). Effectively orchestrating authentication is desired by many, but it’s still in its infancy in the majority of FIs. There are many approaches to achieving this goal—they range from rudimentary to advanced analytics and sophisticated approaches that rely on machine learning. Many executives report that they are overhauling their authentication strategies across all channels, looking for ways to strengthen them, while minimizing customer friction. This is critical when personally identifiable information (PII) is easily available to fraudsters, automated and organized attacks are increasing, and payments are rapidly evolving to become faster or real time.

It may be difficult and expensive to devise such orchestration in-house. Knowledgeable resources are required to design the orchestration across all delivery channels, ensuring a good customer experience while layering security controls effectively. Significant IT resources will likely be required since multiple FI systems will be impacted. A solution provider can offer such orchestration, reducing the time required to bring the functionality into production. One FI executive recently shared that he was able to significantly reduce his FI's application fraud while simultaneously reducing the time required to manually review applications by over 200% compared to the process in place prior to implementation. Such results demonstrate the power of orchestration as well as the dual benefits of reducing fraud losses and operating expenses. Orchestrating authentication for both applicants and existing customers can produce such benefits in many FIs while also providing a great customer experience.

GBG