Banking Application Fraud: The Enemy at the Gates

“It is a fraud to borrow what we are unable to pay.”

– Publilius Syrus, first century B.C.
Contents

Overview................................................................................................................1
What Is Application Fraud?....................................................................................1
The Current Application Fraud Landscape..........................................................2
Types of Application Fraud ....................................................................................2
A Solution to the Problem.......................................................................................3
    Connecting the dots; creating multiple levels of detection..............................3
    Using analytics to find both the known and the unknown risks......................4
SAS® Can Help.......................................................................................................5
What’s Next for Application Fraudsters?..............................................................5
Learn More ...........................................................................................................5
Overview

Fraud is an ever-increasing problem for our financial institutions. Criminals use a wide variety of methods to attack organizations across channels and products throughout the customer life cycle. This paper examines the methods used by criminals at origination, the earliest point of the life cycle, known as “application fraud.”

Inconsistencies in applications – be they credit cards, loans, mortgages or current accounts – can range from innocent oversights, such as an incorrect address, to more deliberate misinformation, such as inflated income details. Organized fraud rings exploit banks that overlook such “minor” inconsistencies because they are becoming increasingly harder to spot among the bank’s normal customers.

Banking application fraud is a critical problem to address as it directly affects a financial institution’s profitability, its customer experience and its bad debts. Conservative estimates suggest that 8-10 percent of a bank’s bad debt book has been misclassified as bad debt when it is actually fraud. These levels demonstrate that application fraud is truly the enemy at the gates, and detecting fraud at the point of application can be the best strategy for reducing these types of fraud losses.

What Is Application Fraud?

Application fraud perverts the traditional challenge of credit risk from the “can’t pay” to a “won’t pay” paradigm. The critical weakness of credit risk-type defenses is the presumption that an applicant is a real person with a single identity as opposed to a fake person with multiple identities. In fact, it’s the criminal’s access to new identities, either stolen or fabricated, that affects a bank’s bottom line.

What started out as check fraud – made famous by popular films such as Catch Me if You Can – has developed into a sophisticated business that operates against multiple points of vulnerability within a financial institution. By its very nature it is often opaque and commonly misrepresented.

Over the last few years, lending banks have improved their level of understanding of application fraud. In countries such as the UK, where institutions have invested in new front-end detection systems, there has been an evolution in how first-party fraud manifests, with the criminals targeting later stages in the customer life cycle. Application fraud, typically seen six to nine months after account opening, is also known as “sleeper fraud” or “bust-out fraud” to reflect the delayed, but then sudden, nature of the withdrawal of funds.

Where application controls still remain weak, and where it is easy to gain access to credit products from day one, fraud continues to threaten at the time of account opening. This issue can be addressed in tandem with an application fraud solution by introducing the concept of constant rescoring of customers post-application.
The Current Application Fraud Landscape

PwC’s Global Economic Crime and Fraud Survey 2018 revealed that, in 2017, 49 percent of global organizations said they’d been a victim of fraud; this is up from 36 percent in 2016. Assumptions are that this number is likely higher. Today companies face a perfect storm of fraud risk, primarily from internal, external, regulatory and reputational fraud. And ever-changing fraud tactics make it hard for organizations to gain ground. Too few companies are fully aware of the fraud risks they face, or even if they’re victims.

For financial institutions, the financial crisis of 2008 resulted in a shift of priorities toward responsible lending and a tightening of credit criteria. Since bad debt (impairment) numbers are now often seen as the general barometer of a financial institution’s health, application fraud has been placed firmly at the top of the agenda. However, the impact of tighter controls cannot be measured by fraud savings alone. Those organizations with the most sophisticated systems deter fraudsters from attack; the least-prepared banks are instead targeted. Furthermore, the reputational impact cannot be overestimated. Financial institutions must be seen as a safe haven, something many are fighting to achieve at the moment.

One of the key challenges with application fraud is separating credit risk underwriting from fraud. Traditional credit scoring models are typically poor at identifying fraud, especially where the fraudster imitates a good credit customer.

Many application fraud systems put in place in the early 2000s are no longer effective. They rely solely on rules and consistency matching, with fraudsters becoming adept at recognizing their limitations. Organized criminals are even prepared to risk discovery of some of their accounts to test thresholds. Fraud managers have acknowledged that legacy systems don’t help with identifying the vast majority of application fraud. As a result, institutions are investing in improved solutions to provide a holistic view of fraud across the entire organization.

These new specialist fraud solutions use sophisticated analytical techniques, combining automated business rules, anomaly detection, predictive models and advanced social network analysis to help solve the problem of application fraud. We’ll explore this approach later in the paper.

Types of Application Fraud

Application fraud can take many forms, but the results remain the same – a financial loss to the organization. Traditionally application fraud is at the first-party level, where the fraudster is the customer. In one such modus operandi (MO), organizations sometimes allow loan applications to be approved and funded in the same day. In this situation, the funds can disappear as soon as the credit arrives in the fraudster’s account.

Application fraud can also occur at a later date (bust-out fraud), where there is an acceleration in activity in a short space of time. The fraudster takes the organization for all possible credit (through schemes such as drawn on uncleared funds, this can be over 200 percent), and then ceases to be contactable or repay any outstanding credit. An example of such a scheme is where fraudsters use their gold or platinum check

---


www.pwc.com/fraudsurvey
guarantee cards to continue to write high-value checks, even after the account has been blocked and closed. Other examples of bust-out MOs can include cash cycling (moving funds around to simulate a good customer) to allow fraudsters to improve their credit rating and maximize the stealing of funds.

A significant issue with application fraud is accounting for fraud losses and how they’re absorbed by an institution’s bad debt portfolio. Typically, anything between 5 and 20 percent of a bad debt will contain first-party fraud. Often banks fail to address a fraud problem by solely using credit risk methods and counteracting early bad-credit accounts; whereas in reality, it is actually first-party fraud and requires a very different approach.

Application fraud can also occur at the third-party level, where the fraudster steals the identity of a customer and applies for a new credit product. This type of fraud is often only identified by the organization when genuine customers realize their identities have been compromised and call to deny knowledge of a credit application. Typically, as much as 40 percent of application fraud can be third-party fraud.

Finally, another serious challenge for banks is third-party online banking fraud and financial crime. A sophisticated application fraud platform can be used to prevent the proliferation of accounts that could be created in support of other fraudulent or criminal activities, such as creating mule accounts for removing money from an online account takeover or for the purpose of money laundering.

A Solution to the Problem

The ability to analyze large volumes of data quickly has progressed exponentially in recent years. With the development of high-performance analytics and in-memory processing, fraud detection systems should now look past traditional rules-based approaches and use the data they have to its full potential. The following section examines some of these techniques in more detail.

Connecting the dots; creating multiple levels of detection

Joining your data together in an intelligent way and using that holistic view for risk assessment maximizes the opportunity to identify fraud patterns and other suspect behavior.

The first level of detection for fraud scoring is at the simple event level, where an event represents an action completed by a customer or even an employee. This could be the submission of a new credit application or a financial or nonfinancial transaction. Each event can be analyzed in isolation, with rules trained against the specific data that makes up the event, to look for warning signs of potential fraud, e.g., an application having a high salary relative to age.

The second level of detection is the entity level. An entity can be any object, such as a person, a telephone number, an IP address, an address or an email. This information can be extracted from the event data and resolved to show a holistic view of each one based on the historical data available. These entities can be assessed for risk in their entirety, allowing multiple attributes to be compared to identify potentially high-risk warning signs, such as identity manipulation, or inconsistent salary and liability information.
The final level of detection is at a network level. Social network analysis (SNA) is a relatively new tool that’s been used for fraud detection since the mid-2000s, and has been very successful in identifying fraudsters at the point of application. Networks are automatically generated where, for example, two applications share an address or telephone number, or where a group of accounts regularly transact with each other. SNA is not simply an analytical technique; rather, it joins data together in an intelligent way, through the application of both direct and “fuzzy” matching, allowing you to identify relationships that would otherwise remain hidden. All possible links between entities can be established, providing a complete networked intelligence view of all the data in an organization, which can then be analyzed for the warning signs of fraud, e.g., a network of individuals with high cash usage and a lack of normal spending activity.

By combining these three levels of detection, an organization can gain a holistic view of its risks and develop proactive fraud management strategies.

Using analytics to find both the known and the unknown risks

Having created a holistic view of customer activity, we can now look at the hybrid of analytical techniques that can be used to identify fraud. These techniques can vary in complexity, but when used appropriately can significantly improve fraud detection rates. An example of a simple business rule could be that the customer age is less than 21 with an income of $100,000. If we were to translate this to an anomaly, it would be that the customer has a very high income in relation to peers, based on the financial institution’s own data or national averages.

**Business rules and anomaly detection**

Application fraud prevention often begins with business rules, which can be written to flag an application. Anomaly detection is more advanced and uses statistical significance to spot abnormal behavior using statistical techniques such as standard deviation or clustering.

**Random forest**

These statistical trees can be used to predict human behavior, including fraud. At each node in the tree, a yes/no decision is realized, and this flow can be used for setting strategies. A random forest is built by using hundreds of different decision trees, taking random samples of the same data using a technique known as “bootstrapping.”

**Logistic regression**

Once a bank has sufficient fraud data volumes, a logistic regression model can be built to predict fraud. Using differential statistical methods, fraudulent customers are separated from genuine customers by a score. Logistic regression is also often used in credit risk to determine bad debt.
SAS® Can Help

SAS has worked with more than 3,100 leading financial institutions across the globe, advising and assisting in their anti-fraud initiatives. Today, more than 90 percent of the top 100 global banks use SAS.

By implementing a hybrid approach to analytics with SAS fraud solutions – including artificial intelligence, machine learning and social network analysis – our customers have realized numerous benefits, including:

- Significant reduction of false positive rates. Clients who were experiencing fraud hit rates of one in 30 are now achieving average hit rates of one in five.
- Increased level of fraud found at the point of application, critically before the money is lost, demonstrating an average ROI of 10-to-1 or more.
- Improved investigator efficiency.

What’s Next for Application Fraudsters?

Application fraudsters continuously share information, work fast and use test-and-learn techniques to probe systems for new vulnerabilities. For example, if an organization used a simple rule for customer age and income, it might generate an alert if the income is greater than $100,000 and the age of the customer is under 21. A fraudster who has worked out both these thresholds will quickly start to submit applications showing an age of 22 and with income of $99,000. Fraudsters often recycle their identities, and this leads to first-party application fraudsters having similar profiles in terms of geography and personal demographics.

As new application channels increase in use (e.g., mobile), new fraud opportunities present themselves, and anonymity becomes easier. The issue is that if financial institutions’ fraud detection tools remain static, they can be exploited by the fraudsters who quickly identify thresholds and take advantage.

To stay ahead of the curve, organizations need a hybrid solution that uses different analytical techniques to identify both known and unknown patterns, yet one that can evolve and adapt with time. This provides a robust solution that eliminates the vulnerabilities fraudsters are looking to expose, therefore deterring the enemy at the gates. The fraudster will only then move on to easier prey.

Learn More

To find out more about how SAS can help your organization with application fraud, visit sas.com/fraudfinancialcrime.