Fraud Protection & Compliance
Application Fraud

WHITE PAPER

FICO®

The changing face of application fraud

New attack vectors, evolving customer expectations, and data proliferation—is it time for a new strategy?

Introduction

Management of application fraud has traditionally been a staid affair. Rules and scorecards have been successful for many years, but we've reached an inflexion point. There are too many changing factors, and organizations that continue to rely on rules, credit bureau data, and batch processing will increasingly struggle to stem the flow of application fraud. Huge data breaches, an increasingly digital economy, and customers who demand instant service call for a new strategy.

Financial services companies are involved in a constant battle to stay ahead of criminals who fraudulently open accounts. This arms race is often limited to incremental changes that are reactive to attacks. In recent years, the factors influencing application fraud have undergone massive changes. This paper looks to establish why now is the time to make a big step up in how you fight application fraud rather than sticking to a strategy of reactive, incremental changes.

This white paper looks at the drivers that forward-thinking fraud departments need to consider, including:

New vectors of attack

Proliferation of consumer data

Increasing customer expectations

New vectors of attack

Constant change in methods of fraud is nothing new, but the variety of factors affecting where and how fraud is carried out have never been greater. Criminals have become more organized, adopting similar business strategies to the businesses they attack. At the same time, they need to be agile to stay ahead of detection, evade law enforcement, and take advantage of whatever low-hanging fruit is available. As fraud is tackled in one area, the fraudsters shift their attention to another, and they are developing their use of technology to stay one step ahead. This means they aim to commit more fraud faster and access and distribute funds before financial institutions can respond.

Developing a robust response to application fraud in a constantly evolving fraud landscape means that financial institutions must identify and be responsive to a wide range of factors.

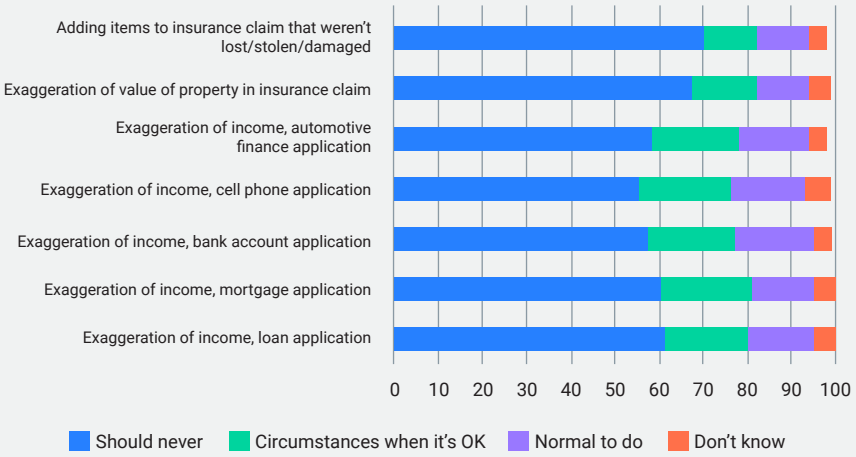
First-party fraud has become more attractive

In some cases, fraud is committed by individuals opening accounts to either access credit they never intend to repay or to use for other criminal activity, such as money laundering. In other cases, people may intend to repay but are dishonest in their applications and obtain funds they wouldn't otherwise get, and their circumstances won't allow them to repay.

While many fraudsters are as brazen as ever and will happily commit fraud in branch, there are more channels than ever before. People can sign up for accounts, online and in the comfort of their own homes. Online services and apps enable them to apply for a wide range of unsecured finance, such as personal loans, quickly and easily. This is a great temptation both for those who plan to commit fraud and for those who lie about their circumstances. From behind a screen, it is easy for people to convince themselves their crime is victimless, and many who would not commit fraud in a face-to-face environment will do so online.

A recent FICO survey found that many people are accepting of behavior that financial institutions would consider as aspects of first-party fraud. For example, across all 14 countries surveyed, 19% think there are circumstances when it's OK for people to exaggerate their income on a loan application, and 15% think it's normal behavior to do so.

What are your attitudes toward the following behaviors?



Results from independent survey commissioned by FICO July 2022. Results average across 14 countries and 14,000 respondents.

COVID, cost of living increases, and a possible global recession may prove to be the stress factors that push even more people toward fraud. In these circumstances, what starts out as a small falsehood on an application form can rapidly escalate to an inability to pay.

It can be argued that the implications of committing first-party fraud are not as significant for the fraud department as other types of fraud. Because the criminal activity comes after an apparently legitimate application, it may appear to be more of a credit risk than a fraud issue. If it is recognized as fraud, it's likely to be in the collections and recovery process. For financial institutions, this is doubly problematic as they are unlikely to collect the funds but will incur significant costs trying to do so. For the criminal it means they are seldom forced to confront their behavior and so are not deterred from attempting fraud again.

Previously, financial institutions expected that their lending portfolios were the main target for fraudulent applications. The advent of real-time payments makes current or checking accounts attractive targets for criminals and extends the range of accounts organizations must protect. These accounts are used by criminals to move funds quickly and ahead of law enforcement, but to do this effectively they need access to many more accounts. As real-time payments gain traction in geographies such as the USA, Canada, Europe, and Australia, it is likely we will see more account applications from those being employed by criminals to act as mules.

Criminal gangs are manipulating people to open accounts for their use. In February 2019, Santander in the UK said it closed about 24,000 accounts in the previous year on suspicion of fraud. About 11,000 of those were suspected money mule cases. Criminals who want to launder money are recruiting people wholesale to open accounts that can then be abused for criminal enterprise. Europol—the European-wide crime enforcement agency—reported in a global study that "newcomers to a state, the unemployed, and people in economic distress often feature among the most susceptible to this crime. This year, cases involving young people selected by money mule recruiters are on the rise, with criminals increasingly targeting financially distressed students to gain access to their bank accounts."

Criminals take innovative approaches supported by technology

Just as legitimate businesses are supported by their supply chain and partners, so are criminal enterprises. This means that different aspects of a criminal enterprise can be outsourced to specialists. An example of this is the use of call center operations set up specifically for criminal purposes. They can carry out activities such as using social engineering techniques to enrich data already obtained through a breach so that it is more convincing when used in an identity theft and subsequent fraudulent account opening.

Criminals are constantly looking for new avenues of attack where they can focus their energies. They can switch their targets because of large changes; for example, the introduction EMV in the USA has led to a spike in card-not-present fraud. Similarly, the introduction of strong customer authentication through the EU's Second Payment Services Directive has made application fraud more attractive as transactional fraud becomes more difficult to commit. Small changes can also be a cue for the fraudsters to act; for example, if a bank targets a new customer segment, introduces a new product or offers a new channel, fraudsters will test the systems for weaknesses. As one provider improves their security, fraudsters turn their attention to another where they find fraud controls to be less robust.

Once targets have been identified, fraudsters have access to sophisticated tools to help them make their attacks more productive. This has been particularly significant in the digital age with more applications made online. Once an organization has been found with vulnerable fraud controls, criminals use technology to multiply the losses with blitz attacks involving the automated submission of mass applications. They industrialize the application process so that it is automated and fast. Many organizations are unable to detect the new attacks fast enough. When they do eventually identify them, they can't modify and adapt their defenses quickly, so losses mount before they can respond.

Today, providers have many more channels to protect, and protection can't be allowed to slip behind for any of them. Care must be taken that in the drive to secure digital channels others aren't left open to attack. With the fraudsters constantly testing for weaknesses, they could suddenly switch attention to an in-branch or postal application process. If data about known frauds is siloed—for example, if the identifying factors of a fraud detected in one channel are not shared with those protecting another channel—this intelligence cannot be used to inform their anti-fraud strategies. There are many cases where banks open accounts where application details such as email address or phone number have already appeared in known frauds.

As previously mentioned, the agility of fraudsters means that organizations are constantly seeing new types of attack. These "zero day" attacks are difficult to spot. Reliance on comparing cases to historical data (such as bureau data) cannot help identify them. Self-learning, machine learning models that can identify fraud based on the behavior exhibited within the fraud are needed to stop it at the earliest possible point before losses mount.

To respond to the volume and threats from first-party fraud, the application fraud process must evolve.

Traditional approach

- Identity theft and synthetic identities treated as fraud issues but first-party fraud treated as credit-risk problem
- High volume of fraud missed pre-book and then not addressed until losses mount
- Identify fraud based on past known behavior

New approach

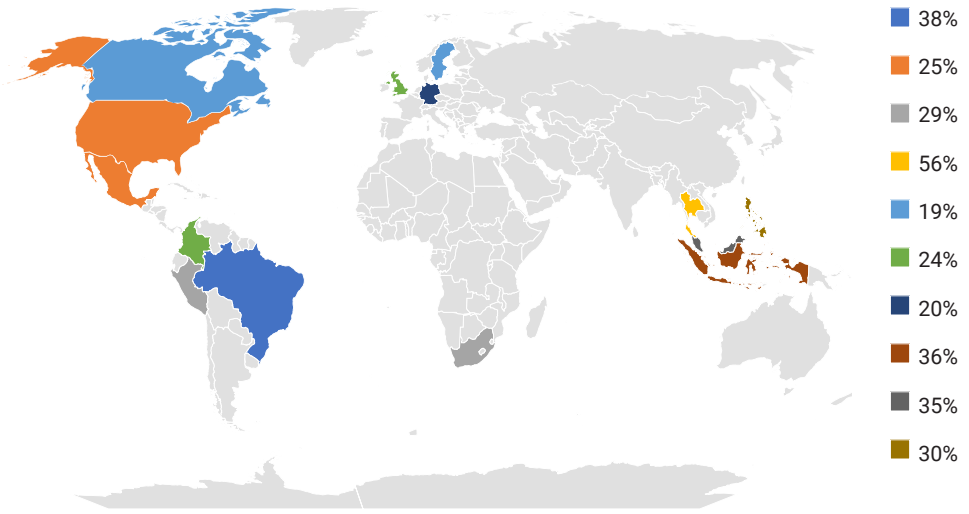
- All fraud treated as a continuum across credit-risk and fraud with co-ownership
- Address more cases pre-book and then address fraud across the customer lifecycle
- Use machine learning models to detect suspicious behavior, even if it hasn't been seen before

More demanding customer expectations

In the digital era, customer expectations have changed and continue to evolve. People expect to have more choice with faster, smoother interactions, and this extends to opening financial accounts. While consumers have high expectations of the service they receive, the financial institution must also be expected to protect the business, the customers, and society in general from fraud. This involves a constant balancing act to keep fraud rates low and customer satisfaction levels high.

To provide an understanding of consumers' attitudes toward the impact that fraud and security checks have on them during the application process, FICO commissioned an independent survey across four European countries. In every country, all respondents were prepared to open at least one type of financial account online. The most popular types of online account openings were for credit accounts or checking accounts (or national equivalent). The least popular types of accounts to open online were mortgages or car loans, but even here, about 20% were still prepared for a digital account opening.

% that have abandoned opening a personal bank account because of difficult or time-consuming identity checks



Results from independent survey commissioned by FICO July 2022. Results for 14 countries and 14,000 respondents.

Applicants don't like online applications to be disrupted

We asked respondents if they had ever abandoned opening an account because identity checks were too difficult or time-consuming. Looking across a number of different account types the results were remarkably consistent with about a quarter of respondents saying they had abandoned an application process. The account type with the most abandoned applications was a personal bank account such as a current/checking account (or national equivalent) where 30% say they have abandoned an application.

People expect to complete online account applications quickly

We wanted to know how long people thought it should take for them to complete an application for a variety of financial products. It's evident that in most cases they expect to complete it very quickly. Numbers for people who are happy to spend over three hours opening any type of financial account were very low. In many instances, people expect to have completed their account application in under 30 minutes.

Traditional approach

- Limited or no cross-referencing of suspicious behavior across channels or products
- Siloed fraud strategy for each channel or product
- Reliance on fraud detection through comparison to known fraud

New approach

- Seamless sharing of intelligence across the enterprise
- Enterprise-wide fraud strategy
- Self-learning machine learning that quickly identifies novel attacks

Meeting customer expectations

The FICO survey shows that customers have relatively high expectations when it comes to opening accounts, and this gives providers several issues to tackle. The pinch points where the need for protection clashes with customer expectations are:

Establishing customer identity. At application, organizations need to be sure the identity presented to them is that of a real person and that it belongs to the individual applying. They also need adequate confidence about other customer information such as address and age. Legitimate customers, of course, know who they are and can become frustrated if they are made to jump through hoops to prove it. Organizations must consider how they can establish identity online in ways that are slick and easy for the customer, don't unacceptably increase their risk, and are compliant with relevant legislation. In recent years, many new identity solutions have come to market, including biometrics. Applying a one-size-fits-all approach to digital identification, however, is problematic—what if your customer can't or won't use your preferred method? Financial services companies therefore need to deploy identity solutions flexibly and should focus not only on what solutions to acquire, but also on how they orchestrate the identity methods available.

Setting up authentication. Once you have established the identity of your customer, you also need to make sure you can easily determine that it is still your legitimate customer every time they interact with you. This may mean collecting additional data from them or asking them to undergo various processes, such as biometric scans, secret information gathering, distributing security tokens, or collecting information about their devices. Providers must balance their need to be able to identify returning customers with a customer's own preferences and tolerances for processes that lengthen the application process.

Traditional approach

- Limited focus on keeping application processes in channel
- Fraud KPIs focused on fraud detection
- Disparate systems for know your customer, credit onboarding, and customer communications

New approach

- Delivery of application processes completely within customers' channel of choice
- Fraud KPIs focused on detection and false positive reduction
- Single platform to effectively orchestrate all solution providers and incorporate the data from them in accurate decision making.

Misidentifying legitimate applicants as potential fraudsters. Commonly referred to as false positives, this is when a legitimate applicant is flagged for investigation because it seems that they might be a fraudster. When this happens, the investigation will either slow down the application, or stop it all together—not a great experience for genuine customers. Providers should focus on managing false positives by:

- Focusing on reducing the rate of false positives by using a range of data and analytics that are more accurate in determining only real cases of fraud. This can be particularly important when faced with new types of attack. Machine learning models that are informed with exemplars of legitimate as well as fraudulent behavior can be key in driving down false positives in applications. Using adaptive analytics, where machine learning models evolve to accurately spot new anomalous behavior, is key to maintaining low false positive rates when new attack types occur.
- Developing strategies for marginal cases. These are the least likely to be fraud. For example, if everything in an application looks correct except for minor differences in how an address is spelled compared to proof documents, while less likely to be fraud, a decision must still be made. It is necessary to identify such cases quickly. These are the cases where it is most important for an organization to understand its own risk appetite and be able to apply proportionate strategies—for example, to consider how light touch and fast the next action needs to be in order to get those likely to be legitimate back on track rather than risk turning a good customer away.
- Streamlining the investigation process. For cases that don't turn out to be fraud, any negative impacts of the investigation must be countered as soon as possible. By using automation and effective customer communications, it's possible to not only get applications on track but to give customers a good experience of being protected.

Traditional approach

- Limited focus on keeping application processes in channel
- Fraud KPIs focused on fraud detection
- Disparate systems for know your customer, credit onboardng and customer communications

New approach

- Delivery of application processes completely within customers' channel of choice
- Fraud KPIs focused on detection and false positive reduction
- Seamless integration between solutions to make customer experience consistent

Data proliferation

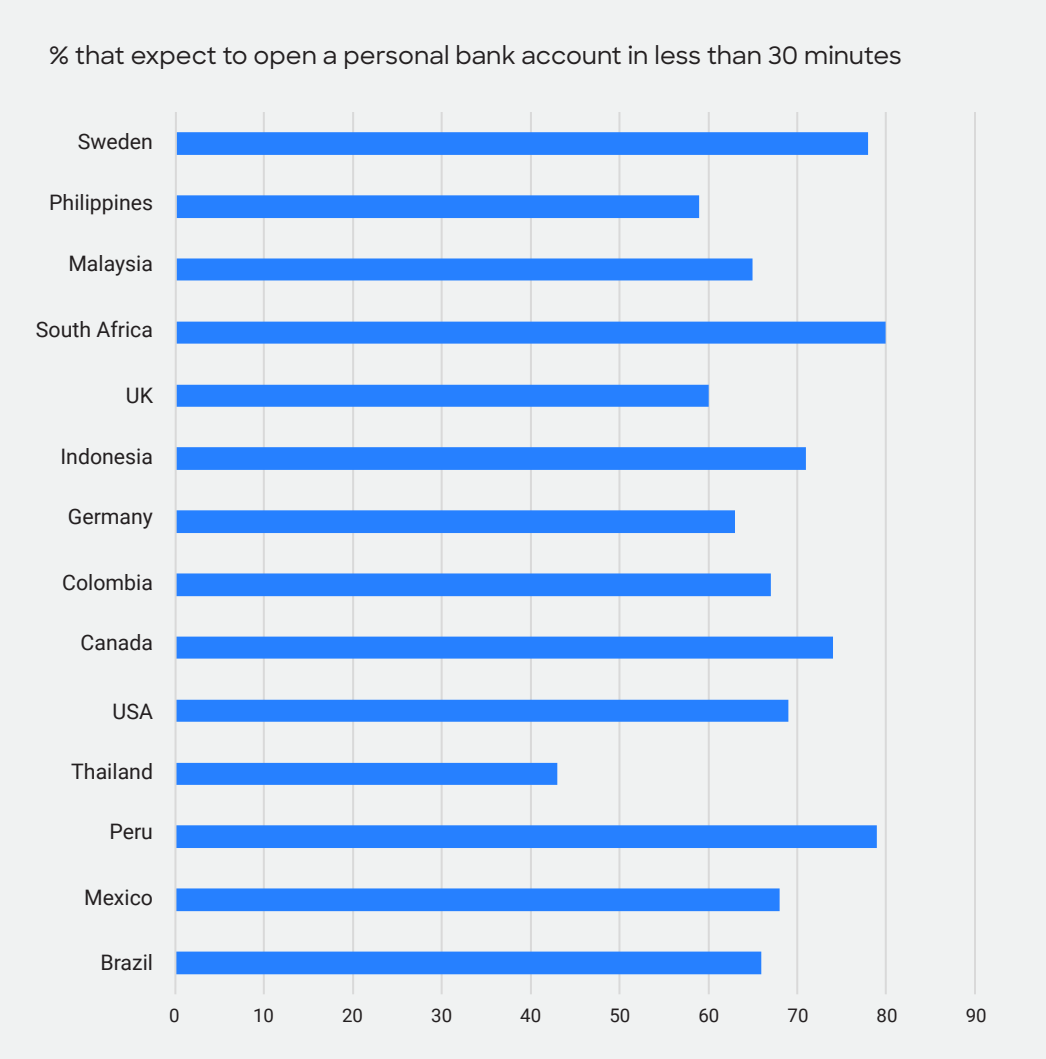
The availability of data can be both a negative and a positive aspect of fraud management.

- Organizations have access to more data—but so do the criminals.
- Decisions can be better informed by availability of data, but the mass of data can lead to too much noise that makes decision making more difficult.
- Data is an asset but managing it is a responsibility and regulatory burden.

When opening accounts, a data strategy is vital: Not only do you need data to ascertain that an application is legitimate, it is often the point where key data is collected about your customer.

Data in the hands of criminals

Constant data breaches and the availability of cheap data for purchase on the dark web make it easier than ever for criminals to steal identities. Providers are then in a constant arms race with the fraudsters to make sure they can't easily use a stolen identity to commit fraud. A 2022 FICO survey of 1,000 people in each of 14 countries found that an average of 10% say they know that their stolen identity has been used by a fraudster to open an account. A further 8% say it's probable, and another 14% say it's likely. In total, this means that a third of people acknowledge that there is at least some likelihood that fraudsters have used their stolen identity to open an account.



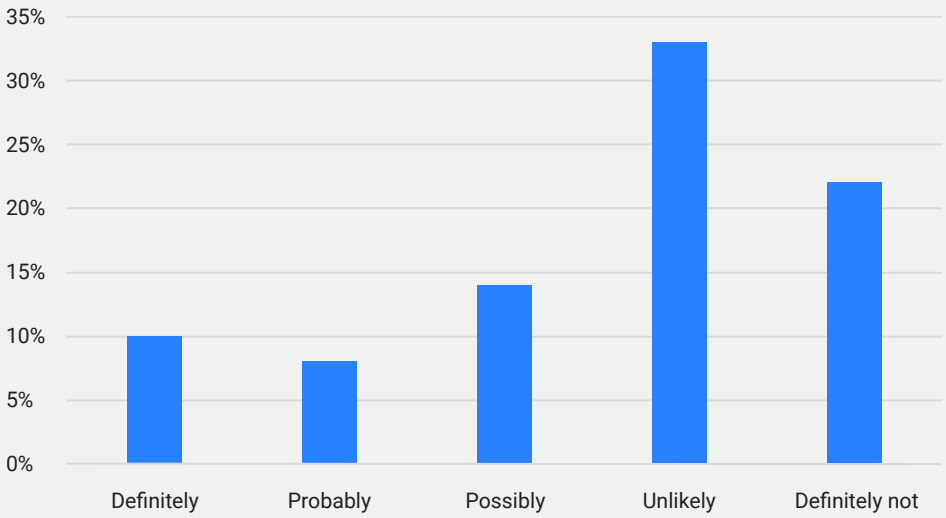
The likelihood of someone's identity being used is compounded by the commoditization of identity data by criminals. On the dark web, records are available for purchase at different amounts dependent on perceived value, and there are discounts for bulk purchases.

Criminals can use elements of data available from data breaches to drive an increase in crime using made up or synthetic identities. Application processes that don't require face-to-face contact make it easier to commit a crime where the purported applicant doesn't exist. The advantage of synthetic identities to the fraudster is that there is no "real" person behind the identity to uncover and report their crimes. The criminals can build virtually unlimited numbers of synthetic identities because there is so much data available to them. This is often a long-term project; they must first build the identities and establish creditworthiness to the point that they can access large sums before they "cash out."

In the US, social security numbers are the key identifier in establishing an individual's identity. Breaches have made these available to criminals; for example, the data breach at Equifax exposed the social security numbers of 146 million citizens. This has driven an increase in the instances of synthetic identity fraud. Social security numbers are issued at birth but rarely used in the context of raising credit until the owner is over 18. Criminals can use the social security number of a minor and combine it with other types of information from a breach—such as name, address, birth dates, and license numbers—to build multiple synthetic identities based around each social security number they have access to. They can then use these synthetic identities to apply for accounts. The sheer number of synthetic identities they can create fuels fraudulent applications at an unprecedented scale. Until 2011, social security numbers were based on a predictable pattern. This meant that given someone's date and place of birth, it was relatively easy for fraudsters to predict what their social security number would be. Since 2011, social security numbers have been randomized. This has prevented fraudsters from easily establishing someone's number and using it to support an identity theft. Conversely, fraud professionals had been using the predictability of a social security number to determine if they had been presented with a fake or real identity, and they can no longer do that.

In other countries, such as the UK, criminals have started to build synthetic identities based on points of entry to establishing a credible identity, for example, setting up accounts at utility companies. Setting up such accounts typically requires minimal or no identity verification, but once such an account is established, it can itself be used to support proof of identity for other products such as a bank account.

Do you think your identity has ever been used by a criminal to open a financial account?



Results from independent survey commissioned by FICO July 2022. Results average across 14 countries and 14,000 respondents

Using data to fight application fraud

Organizations now have access to more data than ever about their customers, however, there are many steps between having access to data and using it effectively to prevent application fraud.

These can be broken down into three main areas:

Data ingestion

This looks at the sources of data and how they are combined. Data can come from many sources, including:

- Data from the application itself (either supplied or metadata)
- Purchased data from third party, for example, a credit reference agency
- Data from third-party identification solutions, e.g., biometric
- Information from previous interactions with the applicant
- Information from records of other accountholders, e.g., common data points such as address, telephone number, or email address

This abundance of data can be a blessing and a curse: It gives you plenty to base fraud decisions on, but any one data element can skew the final results disproportionately. Organizations can struggle with the data they have access to. Those that are siloed and can't share data across products, channels, or stages of the customer lifecycle can end up in situations where, for example, they open an account for a customer whose identity has already been found to be fraudulent by another part of the business. These issues can be particularly challenging for organizations that can't easily and quickly add new sources of data or remove sources that are proving problematic or of limited value.

To make your fraud detection accurate so that more fraud is spotted without increasing false positives, it is necessary to utilize data that not only indicates negative behavior but also signifies what good behavior looks like. It is difficult to get this right. Sources of data from both internal sources and shared, consortia data, such as that from credit reference agencies, provide good references for known bad actors. Conversely, they are unlikely to provide exemplars of what good or normal behavior looks like.

Data enrichment

Having obtained the data needed to make fraud decisions, it is now necessary to organize it so that it will work efficiently and effectively. Dependent on the type and condition of the data you want to ingest, different activities need to happen to make it more usable. For example:

- Making sure there is commonality across sources for structured data—and using the same structure across all data
- Extracting "sense" from unstructured data, for example, by using natural language processing, to identify data elements that are of value to decision making
- Adding context to data, using exemplars to identify data that is indicative of a certain type of behavior such as fraud or non-fraud

Analyzing Data

At this stage, you apply the algorithms and models to your data that deliver actionable insight. The type of models you need to apply depend on the scenarios you face, and in almost every case, a layered approach will be required. The quality of the decisions you can drive from the data you have is determined by the quality and variety of models available to you. For example, if you are facing a new type of application fraud, or an attack on a new channel, models that have been trained to determine fraud through comparison to past attacks will not recognize them. In these scenarios, you need models that are self-learning and can determine outlier behavior that looks suspicious. If you are seeing instances of fraud that have previously been experienced, then models that have been trained using tagged data are valuable.

Conclusion

Generally, we don't make big changes until the cost of doing nothing is outweighed by the advantages of taking the leap. This has meant that systems for application fraud have stagnated with tweaks to existing solutions taking the place of real change. Many organizations have been tied to solutions provided by their data suppliers. Fear of losing tight integration between the data provided and the supplier have made organizations reluctant to take a new approach. But this is no longer the case. As this white paper illustrates, there are many more parameters at play than simply matching application data to known fraud cases. The need for negative data files is still there, but that data can be ingested in today's new solutions and they can also offer myriad advantages where traditional solutions lag, including:

- Real-time detection that doesn't slow or stop applications
- Detection of fraud through positive and negative data examples
- Adaptable suites of machine learning technology
- More automated case management with integrated customer communications
- Advanced fuzzy matching to better identify links across applications and customer records
- Visualization that shows the activity of organized fraud rings
- Flexible ingestion of data assets that can be quickly and easily added or removed as needed

Traditional approach

- Reliance on reference to negative data files
- Single models or multiple models that don't work together
- Inflexible and limited data ingestion

New approach

- Data strategy informed by negative and positive exemplars and negative data files
- Multi-layered analytics that work together
- Advanced data orchestration that is flexible, fast to deploy, and easy to change

How FICO helps

Both pre- and post-book application fraud is a complicated problem. FICO® Platform brings together core capabilities that can aid detection and resolution across the customer lifecycle.

Use all the decisioning data you need
Bring together all the data you need to make informed decisions about your customers' identities and their key attributes. FICO Platform allows you to access, format, and use all internal datasets as well as use preconfigured APIs to use data from your best-in-class third-party identity solutions.

Build actionable insights
Uncover the connections in data across accounts and applications, such as the re-use of telephone numbers in apparently unconnected records, which indicates activity by criminal networks. Apply machine learning and analytics to detect the signals of application fraud using FICO's application fraud models and use FICO Platform to author and deploy your own models.

Take meaningful action
Build rules and decision trees that leverage insights for the best possible outcomes. Adapt rules as new fraud typologies develop without needing specialist support. Orchestrate processes that are appropriate to the scenario; for example, use adaptive workflows that implement identity checks based on level of risk for each application. Configure case management capabilities to prioritize and assign cases and ensure the right information is available for fast resolution. Use multi-channel, two-way communications to keep customers informed, help them to help you resolve cases, and automate information gathering.

Understand outcomes and continuously improve
Create and manage diverse views of data for analysis to better understand and articulate the relative benefits of different fraud strategies. Use simulation to help you test and compare different strategies, identify the best strategies to put into production, and understand the impact they will have on the wider environment before you deploy.

Adapt, expand, and grow
FICO Platform provides the building blocks to tackle multiple use cases. Realize economies of scale by using the capabilities required to manage application fraud across other use cases, for example, to manage your originations and credit risk process or to detect and manage other kinds of fraud. Leverage the advantages of a single architecture to access data and insight across them all to break down organizational siloes, gain a true single customer view, and accelerate digital transformation.

Access domain expertise to accelerate time to value
FICO experts understand best practice, and they can interpret your requirements and advise on your best path forward. They know how to do exactly what is needed and have done it many times before. They can remove the burden from your internal fraud and IT teams helping you to keep resource levels stable and your internal focus on your priorities. Their external perspective enhances your fraud and originations strategies and helps you realize the benefits of your investment as quickly as possible.

Additional Questions?

If you have questions or need information beyond what we've covered in this white paper, please contact your client partner or visit us at

www.fico.com

FICO More Precise Decisions

FOR MORE INFORMATION
www.fico.com
www.fico.com/blogs

NORTH AMERICA
+1 888 342 6336
info@fico.com

LATIN AMERICA & CARIBBEAN
+55 11 5189 8267
LAC_info@fico.com

EUROPE, MIDDLE EAST, & AFRICA
+44 (0) 207 940 8718
emeainfo@fico.com

ASIA PACIFIC
+65 6422 7700
infoasia@fico.com

4721WP_EN 8/22 PDF