

# RISK ANALYTICS FOR FRAUD PREVENTION: TOP USE CASES IN BANKING

WHITE PAPER





## TABLE OF CONTENTS

Executive Summary	3
Fraud Prevention Challenges in Digital Banking	4
Use Case #1: Account Takeover Fraud Detection	6
Use Case #2: Building Trust in the Mobile Channel	9
Use Case #3: New Account Fraud Detection	11
Use Case #4: Removing Friction from the CX	14
Conclusion	16



## EXECUTIVE SUMMARY

The rapidly changing threat landscape is making it easier for malicious actors to commit fraud. The threats banks face are evolving faster and becoming much more sophisticated, with automated attack tools, the emergence of attacks-as-a-service, and close collaboration amongst bad actors enabling financial cybercrime at scale. For executives responsible for stopping fraud, it is becoming increasingly difficult to identify fraud and take action before customers and the organization are affected.

Worse, COVID-19 has made an already challenging situation even more so. Organized crime rings have driven up fraud losses for many FIs, using phishing scams to prey on fear and uncertainty; exploiting higher limits on remote check deposits; deploying mobile attacks to capitalize on the spike in mobile users; perpetrating application fraud; accelerating mule recruitment; and now, targeting government stimulus payments.

Across the industry, losses to fraud already tally into the tens of billions and that is set to increase year over year. While that is a staggering amount of money, the stakes are even higher as research shows that fraud victims tend to blame their financial institution and are more likely to switch.

Trace Fooshee, Senior Analyst at Aite Group and former Head of Enterprise Fraud Strategy at SunTrust Bank, likens the job of today's fraud managers and analysts to *combat banking*. "Those who manage fraud do so under the constant and intensifying siege of criminal activity," he says. "Without sophisticated fraud solutions that constantly re-tune themselves for the purpose of maintaining accuracy and reducing friction, it's going to be increasingly difficult to keep clients safe from attack."<sup>1</sup>

In this paper, we define a risk-based approach as the decision analytics of a fraud prevention system, where a decision engine and machine learning model analyze a broad range of data, events, and context in a continuous way. Based on the risk level of each user action, a risk analytics solution generates a score and provides a recommended next step in real time.

To help fraud managers and analysts better understand the value of continuous fraud monitoring and dynamic risk assessment driven by machine learning – as well as how to enhance existing fraud systems with evolving capabilities – we review the top use cases for risk-based fraud prevention. You'll learn:

- Why risk analysis is foundational to building a great user experience
- Why prioritize server-side analysis of mobile risk signals
- How to identify digital channel attacks before a fraudulent transaction is completed
- How to lighten the load on your fraud team



Today, you need to reduce the liability in terms of the losses and find the financial criminals more effectively



**Trace Fooshee,**  
Senior Analyst at Aite Group  
& former Head of Enterprise  
Fraud Strategy at SunTrust  
Bank

## Fraud Prevention Challenges in Digital Banking

Banks first started deploying rules-based fraud prevention systems decades ago. While fraud teams have relied on rules as the gold standard in fraud prevention for years, they are now faced with the need to modernize as the overall attack surface has expanded dramatically, attack rates continue to rise, and sophisticated attacks are increasingly taking a toll.

Today in the wake of COVID-19, we are seeing a sharp increase in fraud attacks. According to Aite Group, “One large FI executive says that his FI had previously forecast an 8% decrease in fraud in 2020 and has revised that projection to a 10% to 15% increase in fraud for the year, and he says most peer banks have done the same.”<sup>2</sup>

To combat the onslaught of fraud, detection and prevention solutions need the ability to do real-time fraud analysis through analytics. Fraud systems need to be able to look at transaction activity, both in real time and historically, to make instantaneous decisions about fraud.

One of the main challenges for financial institutions has been keeping their fraud defenses up to date. There are a lot of advanced detection and prevention capabilities on the market, but as Aite Group’s Trace Fooshee explains, “It’s becoming more difficult to manage and orchestrate them in such a way that you’re minimizing impact on legitimate clients and maximizing impact on fraudulent clients.”<sup>3</sup>

This is easier said than done. Despite having multiple fraud systems in place, banks and other financial institutions still have gaps in their fraud protection because their multiple fraud technologies were never designed to work together. Similarly, it is not always easy to harness the underlying cross-channel data (especially contact center data) needed to feed a holistic view of the customer’s behavior, because the data is so siloed. However, this data is incredibly helpful in fighting fraud.

As an example, many fraud prevention solutions focus solely on the login and the transaction. However, there are different ways an attack propagates, including where an attacker performs several operations before creating a transaction. If your existing fraud solution only looks at the login and the transaction, it may have missed all of the behaviors that led to that transaction. Consider a scenario where the user’s account has been taken over, the fraudster has provisioned a new device, and they have used the call center to change the contact phone number or email address, in order to keep the legitimate account owner from receiving notifications from the bank. That context is essential to preventing the account takeover. This requires the ability to monitor and analyze the data related to sessions, users, devices, behavior, and all of the events that users perform in a banking application – in real time, as they occur – to determine the probability of fraud.

In addition, shortcomings in orchestrating the fraud tech stack and harnessing data can also result in a disjointed client experience. Ultimately, fraud teams face a delicate balancing act in almost every decision they make. They must reduce fraud losses, deliver a great customer experience, and meet regulatory requirements – all while trying to contain costs. There is a better way: leveraging risk analytics as a core technology and the resulting risk scores to apply precise security for each transaction. This way, FIs can manage security risks without shifting the burden to the customer.

“Today, you need to reduce the liability in terms of the losses and find the financial criminals more effectively, but in doing so you’ve actually got to improve the client experience,” says Fooshee.<sup>4</sup>

Ultimately, that is the value of real-time risk analysis in fraud prevention. A risk analytics solution must be able to understand the risk at every moment in the customer’s digital banking journey, and respond in real time.

To achieve this, the risk analytics system should analyze all user events (e.g., a login, a change in user profile, adding a payee, a change in access permissions, a financial transaction, etc.). For each event, the system must analyze the attempt, the authentication, and the outcome. By reviewing all of these within a digital banking session, the system will understand how events are connected and identify combinations of suspicious actions.

Finally, such a system should also compare the customer's current behavior with their previous online and mobile banking sessions, as well as analyze how the customer is moving across digital channels and devices (e.g., are there locational anomalies; has the user been phished; is there malware on the device?). All of this analysis can happen behind the scenes, protecting the customer without having an impact on the user experience.

**Figure 1.** Challenges underpinning the need for risk analysis in fraud prevention

CHALLENGE	HOW TO...
<b>Reduce fraud</b>	<ul style="list-style-type: none"> <li>• Detect new account fraud</li> <li>• Detect fraud resulting from account takeover</li> <li>• Identify and counter new attack scenarios</li> <li>• Efficiently deal with attacks that continue to grow in volume and complexity</li> <li>• Build a comprehensive anti-fraud framework</li> <li>• Combat the increasing volume and sophistication of mobile malware</li> </ul>
<b>Optimize both user experience and security</b>	<ul style="list-style-type: none"> <li>• Ensure that customers see your organization as security-conscious</li> <li>• Evaluate risk and inject additional security measures only when necessary</li> <li>• Avoid a one-size-fits-all approach to authentication</li> <li>• Perform behavioral profiling on users, devices, payees, and locations</li> </ul>
<b>Build and maintain trust</b>	<ul style="list-style-type: none"> <li>• Reliably assess whether the legitimate customer is performing all actions in the account</li> <li>• Establish and manage trust in the mobile channel</li> </ul>
<b>Reduce costs related to fraud</b>	<ul style="list-style-type: none"> <li>• Find cost efficiencies when maintaining a large fraud team</li> <li>• Automate trust management of users, devices, payees, etc.</li> <li>• Keep the cost of regular upgrades to the anti-fraud tech stack under control, while still ensuring the ability to detect emerging attack scenarios</li> <li>• Avoid fines for non-compliance</li> <li>• Avoid the cost of poor user experience and abandonment</li> <li>• Avoid indirect costs related to reputational damage and lack of trust</li> </ul>
<b>Meet regulatory requirements</b>	<ul style="list-style-type: none"> <li>• Comply with increasingly complex regulations and a diverse patchwork of regulatory considerations, based on the countries in which you operate</li> </ul>
<b>Keep up as security evolves</b>	<ul style="list-style-type: none"> <li>• Keep up with new areas of security expertise, e.g. mobile app security, device intelligence, session monitoring</li> <li>• Effectively leverage threat intelligence while managing overwhelming volumes of data related to apps, devices, users, accounts, and channels</li> <li>• Connect risk capabilities and share data across business lines and functions</li> </ul>



## Use Case #1: Account Takeover Fraud Detection

Account takeover fraud happens when criminals gain access to the victim's personal and financial data in order to steal funds or cause other forms of damage. Fraudsters have a variety of techniques at their disposal to achieve this, such as phishing, malware, man-in-the-middle attacks, man-in-the-browser attacks, social engineering, and victim-assisted compromise. Because account takeover can be committed in many ways, it is, as Aite Group notes, "a peculiar and particularly unsettling form of attack, and one that has evaded a standardized definition."<sup>5</sup>

Due to the number of methods that criminals can use to gain access to their victims' accounts, it is difficult for FIs to build an efficient system to thwart all possible account takeover scenarios. Industry publications constantly report on new attack vectors, but even well-known techniques continue to yield profits. It's not something FIs can fully control since the risk is distributed between the bank's anti-fraud systems and their customers' devices and actions. Looking at how risk is allocated, it's no wonder that this type of fraud remains one of the top concerns among fraud executives, according to an Aite Group survey.<sup>6</sup>

While attack techniques vary in sophistication, many are perpetrated by cunning and motivated cybercriminals backed by organized crime groups. No one is immune and the reality is the losses to account takeover continue to grow. In fact, the "2020 Identity Fraud Report" by Javelin Strategy & Research found account takeovers trending at the highest loss rate to date, up 72% in 2019.<sup>7</sup> And while FIs and industry analysts are not seeing a new surge in account takeover attacks as of publication of this paper, once criminals have depleted their opportunities to profit from stimulus fraud, analysts expect to see more account takeovers. "All of the indicators point to this, considering the increase in first-time digital banking users; all of the data harvested from pandemic-themed phishing scams; and the increased limits for contactless transactions, for example," says Julie Conroy, Research Director for Aite Group's Fraud & AML practice.

Apart from the human factor, there are several reasons why criminals still succeed with account takeover attacks, despite security steps undertaken by FIs. For one, attack scenarios rapidly evolve and new tools constantly appear on the Dark Web. Traditional anti-fraud systems are based on rules and historical data, and use defined criteria to filter events. They are good at detecting known attack patterns, but fall short of identifying new fraud scenarios. This is a risky situation, leading inevitably to the increase in fraud. Even modern fraud management solutions fail to deliver if their detection capabilities are based on limited data or scope. This can be caused by too narrow a range of data points collected, or because the anti-fraud system only analyzes a select aspect of user activity (for example, only pertaining to current activity on the account). Many banks still use anti-fraud solutions that only look at the payment and therefore don't have enough context to know whether it is fraudulent or not, making them, to a certain extent, blind to what is right in front of them. Instead, they should be looking for potential indicators of compromise with unusual behavior. Often too much reliance is placed on client-side intelligence (i.e., login and transaction) as opposed to server-side intelligence with machine learning. Having a tight integration between the two enables a server-side risk engine to consume vast amounts of client-side device and mobile app integrity data. This is critical to accurate risk scoring.

### Continuous and comprehensive data collection and analysis

Using a combination of rule sets and machine learning, modern risk analytics tools provide the ability to proactively detect signs of an account takeover before it affects users. Such a solution will continuously collect, analyze, and score mobile, application, and transaction data in real time. This way, FIs gain full visibility into



OneSpan recommends an approach based around continuous monitoring and intelligent risk analysis.

The full benefits of the continuous monitoring approach [...] include, but are not limited to, reduced fraud, improved user experience, identifying and reacting to a session hijack, identifying when new devices are introduced to a session, increased real-time intelligence and more.



FinTech Magazine

user activity across digital channels – captured before, during, and after each banking session. This is known as continuous monitoring.

A good risk analytics solution detects patterns in the user, device, and transactional data, which can provide an indication that customers are under attack. Looking at different account takeover scenarios, there are typically clues in the data that a customer may be under attack. These clues are known as indicators of compromise. Examples include malicious headers, referrers from a phishing site, malicious cookies, a malicious device or IP, inhuman speed, keyboard overlay, a debugger running, etc.

To detect signs of account takeover, the data analysis needs to assess several layers:



- 1. Device/Client:** Within this layer, a risk-based anti-fraud system should use device data collectors to profile new and existing devices, identify device changes, and analyze location and contextual data (i.e., the types of data will include device type, OS version, location, etc., and/or whether the app has been tampered with). The collected data elements create a detailed profile and a unique fingerprint of the user's device.
- 2. Behavior and interaction with the device:** The solution should analyze the user's journey across the entire banking session. It should profile user behavior and interaction with the application/device, such as login speed, accuracy of movement, etc. Behavioral biometrics technology can greatly contribute to the data analysis in this layer.
- 3. Analysis of user and account activity on a historical basis:** The solution should analyze past actions and check how well the current behavior matches the historical profile. This can include actions like adding a new payee, time of login, duration of the session, etc.
- 4. Cross-channel and cross-device:** The solution should gather and analyze data to create a full overview of user behavior across digital channels, as well as devices and products.
- 5. Server-side analytics:** The decision engine and machine learning should connect and analyze data from all layers, checking the links between the different users, devices, and transactions, while also considering hotlists such as device reputation and IP intelligence.

This layered analysis makes it possible to identify a broad range of suspicious behaviors (or combination of behaviors) that may be indicators of an account takeover attempt. Examples include:

- **Attacks on the login process** resulting from stolen credentials, mobile overlays with fake login screens, bypassing 2FA methods, etc.
- **Compromising SMS communications:** To circumvent security controls such as strong customer authentication, criminals will use techniques such as SIM swapping where all of the victim's SMS messages (including one-time passcodes) are redirected to the fraudster's phone.



Frost & Sullivan's research indicates that fraud prevention solutions focused primarily on static data and rule-based analytics to address transaction fraud are inadequate for preventing the sophisticated mechanisms employed by hackers. There is a clear need for behavioral analytics-based fraud management solutions that can leverage the power of machine learning (ML) and artificial intelligence (AI) to identify threats and assist with timely decision-making for fraud prevention.



Frost & Sullivan

- **Unauthorized user account profile changes:** As an example, criminals will often try to change the legitimate user's contact details (or other profile changes), make a password change, or make changes to notifications in order to prevent the bank from contacting the legitimate customer.
- **Suspicious funds transfers:** Examples include a sudden change in spending patterns, like a high-value transfer to a new payee, or several payments to a new account in a short period of time.

### Machine learning

Today, the key building block is to complement the decision engine with machine learning and sophisticated predictive modeling. The idea is to prepare for the unexpected, instead of trying to create a rule for everything.

A modern risk analytics solution should have the ability to use machine learning algorithms to analyze vast amounts of data, understand patterns of good behavior, and spot anomalies in milliseconds. It will then require appropriate action based on the risk level.

Machine learning can be used to contrast the user's normal behavior against suspicious behavior, such as the behavior of a bot or attacker. This enables a detailed and accurate analysis of user actions, which in turn allows FIs to avoid unnecessary friction and reduce the number of false positives (non-fraudulent events identified as fraud). In addition, thanks to their strength in detecting anomalies, machine learning algorithms effectively spot new and emerging attack scenarios, which a rules-only system cannot achieve.





## Use Case #2: Building Trust in the Mobile Channel

According to the U.S. Federal Bureau of Investigation (FBI), “Studies of US financial data indicate a 50 percent surge in mobile banking since the beginning of 2020.”<sup>8</sup> A recent Aite Group survey of 2,413 US consumers in Q1 2020 found that 86% of senior millennials, 83% of young millennials, 72% of Gen Xers, 38% of baby boomers, and 17% of seniors log into banking accounts using their mobile phone at least once a week.<sup>9</sup>

Even mobile corporate banking transactions are increasing in volume. Citi reported a tenfold increase in users of its corporate mobile banking app, CitiDirect BE, in March 2020 when compared to the same month a year earlier.<sup>10</sup>

While the recent surge in mobile banking has been largely attributed to COVID-19, this growth in mobile use will continue. Criminals follow opportunity and the path of least resistance. Now more than ever, that opportunity is in mobile. Industry experts report a 37% increase in mobile phishing attacks globally<sup>11</sup> in Q1 2020 compared to the previous quarter, and a 173% increase in mobile banking Trojans<sup>12</sup> for the same period.

The mobile channel has become a top target for attackers, but paradoxically, some FIs claim they don't experience much mobile fraud. It's more likely that the organization is just not able to detect and track it. For example, a mobile overlay attack is designed to capture login credentials. The attacker could then use those credentials to infiltrate the online channel, but the attack originated in the mobile channel. A risk-based fraud system would catch that and stop it before it propagates.

Defending against mobile attacks and building mobile channel trust should be of top concern, as much to traditional banking institutions as mobile-only banks and digital challengers. Not only do consumers want to stay in the mobile channel, mobile is the least expensive and most information-rich channel for a financial institution. Yet according to a Deloitte survey, 52% of consumers want more data security for their mobile banking apps.<sup>13</sup> To enable growth, the financial services industry must keep an ongoing focus on building and maintaining trust in the mobile channel.

Establishing and maintaining mobile trust requires extensive data analysis. It is important to collect, securely communicate, and analyze data that includes elements characteristic of the mobile channel. Capturing only partial data (for example, without profiling the mobile device) will affect the accuracy of the risk analysis.




This is where a risk analytics solution can leverage other tools, such as a mobile device data collector SDK. The data collector can consume a broad range of mobile-specific data, in a transparent and continuous manner. This includes:

Customers have high expectations when it comes to their mobile banking experience. They want their FI to know them as a person, not an account number. They want to know their money is secure. And they want FIs to anticipate their needs and simplify their lives.

FIs can meet these expectations through trust, and in particular, digital trust. Trust in the mobile channel is formed between:

- Users and client applications
- Client and server applications
- Server applications and users

When trust exists between these, FIs can offer an exceptional mobile banking experience.

 <b>USER DATA</b>	 <b>DEVICE DATA</b>	 <b>APP DATA</b>
<b>Examples:</b> <ul style="list-style-type: none"> <li>• Biometric data</li> <li>• Authentication method</li> <li>• Behavioral profile</li> </ul>	<b>Examples:</b> <ul style="list-style-type: none"> <li>• OS version</li> <li>• Device model</li> <li>• Jailbreak/root status</li> </ul>	<b>Examples:</b> <ul style="list-style-type: none"> <li>• Screenshot detection</li> <li>• Code injection alert</li> <li>• Overlay alert</li> </ul>



OneSpan's mobile app SDK supports application shielding for mobile apps as well as collecting device context variables for risk scoring.



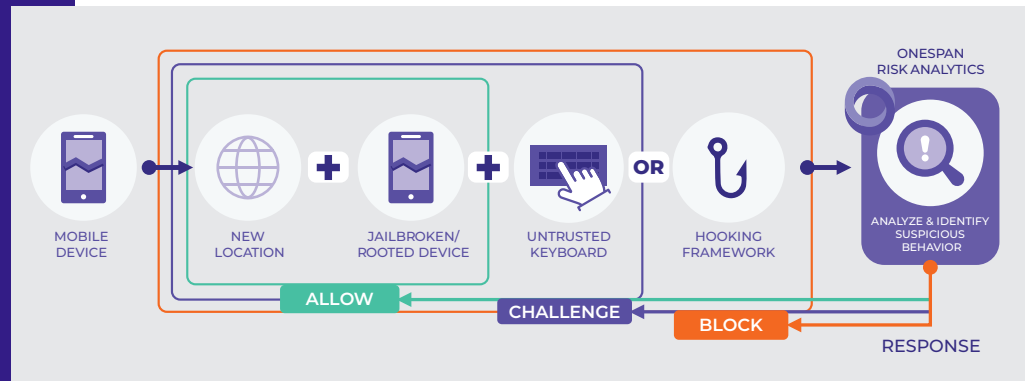
The Forrester Wave™: Risk-based Authentication, Q2 2020

A trusted mobile device enables FIs to expand the scope of services offered via the mobile channel. Continuous evaluation of risk gives more confidence to FIs concerned about sophisticated mobile fraud attacks. With a risk analytics engine, FIs can confidently enable any use case.

A trusted mobile device also supports use cases beyond mobile banking. When an FI applies security measures that allow for the right amount of trust, the customer's device can double as a multi-channel authentication token. It can then be used to securely authorize transactions for online banking.

Additionally, FIs need to establish a secure communication channel, secure storage, and server-side analysis capabilities. This prevents the data from being compromised and enables a device profile to be created on the server side to continuously score the device and evaluate the trust allocated to it. This in turn allows FIs to offer their customers a secure and robust banking experience. The more accurate and detailed the data analysis is, the broader the scope of services that can be offered.

**Figure 2.** Risk Analytics combined with app shielding dynamically adjusts the behavior of the mobile app.



### Best practices

In the mobile environment, the level of trust can change dynamically. FIs have no control over what type of device the customer uses, what is installed on the device, or if the mobile phone has fallen in the hands of criminals as a result of theft or loss. It is difficult to assign a sufficient level of trust to the user's device in these circumstances, which puts the security of mobile banking operations at risk.

This is why it is so important to:

- 1. Dynamically evaluate trust associated with the device.** It is not enough to establish the level of trust when a user begins their banking session. The state and condition of the device can change any minute (e.g., if a user installs a suspicious app). This can create risky circumstances in which neither the FI nor the user is controlling the banking transaction any longer.
- 2. Instantly react to any changes to the environment in which the banking app is operating.** The FI's role is to maintain a live assessment of the situation and to step in immediately when there is a justified suspicion that the device (and therefore the banking session) has been compromised.
- 3. Verify the user's digital identity in a transparent and continuous manner.** In addition to monitoring the environment the banking app is operating in, FIs also need to confirm that they are dealing with the legitimate user throughout the whole session, to prevent a situation in which a bad actor takes over after the user has successfully logged in. The FIs need to look for any clues that the transaction request is not coming from the legitimate user and can do that by assessing the behavioral context.

### Pairing risk analysis with mobile application shielding

All of this begs the question, what should FIs do when the trust level decreases – should they deny access to services? Clearly, a rigid approach to device trust would frustrate a large segment of mobile users. Many mobile devices are jailbroken or rooted. Just the fact that a jailbroken device is being used in the mobile banking channel will raise a flag in the risk analysis. Rather than shutting down the app, FIs can pair their risk analytics technology with [application shielding](#) and mobile security technologies. These technologies optimize fraud management but still allow the banking app to function securely in an otherwise risky environment.



Synthetic identity fraud, where crooks invent realistic-seeming identities out of scraps of real ones (for instance, one person's Social Security number, another's mailing address) has plagued banks for years.

Aite Group estimates this type of fraud costs U.S. lenders \$10,000 to \$15,000 per incident. Auriemma Insights estimates the losses are \$6 billion annually. And McKinsey says 85% to 95% of loan applicants identified as potential synthetic identities are not flagged by traditional fraud models.



American Banker

## Use Case #3: New Account Fraud Detection

New account fraud occurs when a fraudster or a mule has been **successfully onboarded** by a financial institution (FI) after applying using a synthetic identity, stolen identity, or even the mule's own identity. Once they have access to the new account, they will apply for credit, max it out, and disappear.

In the case of a mule account, fraudsters use the account to move funds stolen during a fraud attack. A 2020 article by cybercrime investigative reporter Brian Krebs shared the details of an [elaborate vishing scam](#) that duped a victim out of \$10,000. The attackers then authorized a wire transfer out of the victim's legitimate account and into a new online account that they had opened in the victim's name.

As fraudsters get more aggressive, they continue to leverage identity theft to perpetrate further new account fraud. In fact, 1.5 million victims of account takeover fraud had an intermediary account opened in their name – a 200% increase over the previous year.

How is it possible that fraudsters and mules can open a deposit or credit account without detection?

- When the fraudster is using a synthetic or stolen identity, this often happens because the FI lacks the robust [identity verification technology](#) needed to catch fraudulent identity documents during the application process.
- When the fraudster or mule is using their own identity and authentic identity documents to open a mule account and commit new account fraud, this is much more difficult to catch during the application stage. However, as we explain on the next page, a risk-based fraud prevention system can help thwart **fraud attempts from the account holder's first interaction with the account.**

The challenge for FIs is that failing to catch the fraudster or mule during the application and onboarding stage opens the door to significant risk later on. New account fraud is a growing problem for financial institutions – and a top concern for FIs in the wake of COVID-19. According to an Aite Group report on mule activity, "Evidence suggests that the recent coronavirus pandemic and the global economic recession resulting from this unprecedented disruption will further contribute to an expansion of the labor pool that mule recruiters have to draw from."<sup>14</sup>

**Figure 3.** There are different forms of account opening fraud. While “application fraud” and “new account fraud” may seem like synonyms, they are different.

	APPLICATION FRAUD (detect it before the account opening)	NEW ACCOUNT FRAUD (detect it after the account opening)
<b>Definition</b>	Application fraud is identity fraud that occurs when a <b>new applicant is trying to open an account</b> using a stolen or fabricated identity.	New account fraud applies to fraudsters who have <b>already been successfully onboarded</b> due to lack of identity verification technologies.  Note: New account fraud is not account takeover. In the case of ATO, the owner of the account is the victim. With new account fraud, the owner of the account is either the fraudster or mule.
<b>Prevention best practices</b>	Use <a href="#">digital identity verification technology</a> as part of the remote account opening process. Purpose-built solutions rely on document verification and facial comparison algorithms to detect fraudulent and stolen identity documents. Used together, facial biometrics and digital ID document verification can ensure an applicant is in fact the person they claim to be.  This can also be combined with threat intelligence (e.g., leveraging a risk engine to flag known malicious devices, ISPs, locations, etc., from a blacklist) during the application stage, before accepting the applicant as a customer.	Best practice is to monitor all new accounts closely, especially in the first 30 days when fraud is mostly likely to occur. Risk analytics solutions with behavioral monitoring enable financial institutions to track: <ul style="list-style-type: none"> <li>· dormant accounts;</li> <li>· dormant-to-warmed-up accounts;</li> <li>· high transfers in/out beyond what would make sense based on salary and other data in the customer’s application, etc.</li> </ul>

### Fraud in Digital Account Opening

As the demand for mobile account opening increases, banks and other financial institutions must reduce fraud and losses related to application fraud, account takeover, and synthetic identities. We recently released our [third annual banking survey](#) with Information Security Media Group (ISMG), the world’s largest media organization devoted to information security and risk management. The survey looked at the state of digital account opening transformation. What it showed is that digital banking is in a growth mode. However, in addition to the 80% of survey respondents seeking to streamline the digital customer experience for new applicants, 72% of respondents indicated that they also sought to cut down on incidents and losses related to fraud. In all, 85% reported experiencing fraud during the digital account opening process.

In fact, the survey reveals that **stolen identities** and **synthetic identities** are the top two sources of fraud as a result of offering digital account opening. This is why it is so critical to ensure that an applicant is who they say they are, in this time of low-touch/no-touch interaction.

### Best Practices to Catch New Account Fraud

An anti-fraud solution based on risk analysis provides two layers of protection against new account fraud, and is an important step in detecting anomalies during the onboarding user journey.

The first layer is applied during the onboarding phase, when the new user is registering their device(s) with the bank. For example, when onboarding a new customer, the anti-fraud solution can send data collected during the device registration process to the risk engine to determine whether the device in question has been stolen, whether it was

previously used in a fraud scheme, and more. If the risk engine determines that there is something unusual about the device, it will stop the registration process and flag it for manual review.

The second layer is applied as soon as a new account is opened, in order to study the behavior of newly registered users and devices. For new users, the FI does not have enough information to establish patterns the way they do with existing users. (Although the risk engine will catch a known behavior profile that has been previously identified as malicious.)

However, that doesn't mean the risk engine can't begin analyzing data from the customer's very first interaction with the bank (this can be done during the account opening process or afterwards by identifying suspicious activity during their initial set of interactions and transactions on the account). In this scenario, best practice is to compare the new user's behavior against a representative pool of customers. During that analysis, the anti-fraud system will analyze:

- Spending behavior compared to the average
- Payee profile
- Sequence of actions
- Navigation data related to machine-like or bot behavior
- Abnormal and risky locations
- The account owner's relation to other users

The next consideration is to ensure that the risk engine has the ability to aggregate data on multiple levels. This allows the FI to detect all possible relationships to users, IPs, and devices with proven fraud behavior. That includes information about the:

- User
- Corporation
- Device
- Payee
- Account
- Location
- Session
- And more

If the system notices any unusual changes in the account holder's personal information, the decision engine will flag it as suspicious or indicate that it requires review. It can then be actively monitored and escalated for investigation, if necessary.

As best practice, newly registered users should be monitored closely for a defined period of time until the FI has built a reliable profile and trust level. If the account is inactive or sleeping for a period of time and then the account holder attempts a high-risk transaction, this will be caught by the risk engine. In addition, a risk-based fraud solution should be looking for tactics like warming up accounts, as well as analyzing each payee and detecting mule accounts.



## Use Case #4: Removing Friction from the Customer Experience

Many factors affect customer satisfaction in modern banking. When designing an optimal user experience, financial institutions need to take into account the entire customer lifecycle, from opening an account, through handling daily transactions, to providing quality customer service. According to Forrester, banks should use digital technologies to offer customers “extensive functionality and superior usability across digital touchpoints” as well as “personalized experiences that meet their needs”.<sup>15</sup>

Trust lies at the heart of the digital customer journey. Confidence that the bank controls the security of their actions and transactions is key to a positive customer experience, but financial institutions must also balance security with convenience. Securing transactions cannot happen at the expense of blocking all high-risk interactions, nor can it be done by stacking up security measures for each transaction regardless of the related risk. Providing only selected services through the digital channels, while this might be tempting for FIs with a low appetite for risk, will not provide a competitive edge either, since an increasing number of modern banks are entering the market as digital-only, mobile-first players.

Therefore, when designing customer journeys, it is crucial to secure transactions in a balanced way that is least burdensome for the user. This plays an important role in every aspect of their digital journeys, from allowing mobile banking apps to operate securely in an unsafe environment, to ensuring that the required authorization matches the transaction’s risk level. Ultimately, the goal of an anti-fraud system is to differentiate between users who do and don’t pose a risk – leaving the vast majority to conduct their business and only focusing on the suspicious activity.

Risk analysis is an essential part of this process. Without obtaining and processing enough user, device, application, and transaction data in real time, FIs cannot make informed decisions as to whether a specific transaction should be allowed, secured with an additional authentication challenge, or sent to the fraud analyst for a manual review.

### Reducing false positives

False positives are legitimate transactions that a financial institution’s anti-fraud systems erroneously qualify as fraudulent. This can happen if the risk acceptance threshold is set too low to allow for authorization of transactions with elevated risk (they get labelled as potentially fraudulent). This also happens if the risk analysis is incomplete or incorrect due to:

- A limited scope of data
- A data snapshot from the moment when the transaction took place, without taking into account the context of the whole banking session

Handling false positives will vary depending on the bank’s strategy. This ranges from putting the transaction on hold so a fraud analyst can make the final decision, to denying the transaction. Either way, it results in unhappy customers who, if faced with repeats of this situation, will eventually switch institutions.

A modern anti-fraud solution with an advanced risk engine can help minimize false positives by approaching the data analysis in a 360° manner.

First, data collectors will feed the risk engine with real-time data that covers all aspects of the transaction. This can cover a broad range of data points related to the device used, the customer, their account, and the transaction itself, but also data covering the whole context of the interaction. For example, have they performed similar operations in previous sessions? Or, has the risk level increased during the banking session, e.g. due to a sudden IP change?

Second, this data will be analyzed in an automated manner, using not only advanced rulesets to detect known fraud, but also involving machine learning algorithms to detect emerging fraud. As mentioned earlier in this paper, machine learning can analyze hundreds of different data elements on a historical basis in order to determine the transaction risk score.

Third, a risk analytics solution should not bother users by triggering unnecessary authentication flows for every action they undertake. This means that with a comprehensive approach to risk analysis, fewer of the legitimate transactions will be labeled as potentially fraudulent, which in turn will translate into fewer requests for unnecessary additional authentication.




### Authentication flows that match the transaction risk level

No two transactions are identical, even if they share the same amount, user, and device. Each transaction needs to be placed in context. That can change dynamically, even within the same banking session. Therefore, the modern approach assumes that the choice of authentication methods in the digital channel should be risk-based. In other words, authentication requirements should depend on the transaction's risk score: from allowing a transaction within the existing session without an additional authentication challenge, to applying step-up authentication. For example, if a certain transaction is evaluated as suspicious, due to unusual timing, location of the user, or a significantly larger amount than usual, the risk solution may trigger a scenario to step-up the authentication criteria instead of simply rejecting the transaction or putting it on hold for manual review.

The risk analytics framework can integrate with existing and future multi-factor authentication options. It constantly evaluates risk on a case-by-case basis and, based on this evaluation, can orchestrate the authentication flows in a flexible and dynamic way. It can dynamically trigger the most suitable authentication method based on propensity for fraud, according to the level of risk. It offers flexible workflows, supporting convenient user journeys.

In addition, tailoring the authentication flow to each unique transaction makes it more difficult for fraudsters to predict and plan their attacks. Unpredictability helps thwart a fraudster's attempt to turn a fast profit with minimum effort.

This level of risk-based intelligence ensures the best possible customer experience. From the user's perspective, the usual actions will be seamless; they will not be bothered with cumbersome authentication methods for low-risk transactions. The solution will introduce the right level of friction into the authentication process in order to protect customers' money. This deep analysis never interrupts the user experience unless it is necessary. Instead, users are only impacted when the decision engine determines that the level of risk and propensity for fraud justify it.

 <b>DATA COLLECTION</b>	 <b>RISK ASSESSMENT</b>	 <b>TAKING ACTION</b>
<p>Leveraging data collectors, the risk analytics solution obtains comprehensive data on the integrity of the device and mobile apps, user behavior, transaction details, and other key contextual data across all digital channels.</p>	<p>An advanced risk analytics engine analyzes and scores risk for each transaction. The combination of pre-configured rules and machine learning provides the best method to detect both known and new fraud techniques.</p>	<p>Paired with a risk-based authentication module, the risk analytics solution can trigger the most appropriate action. Higher-risk transactions will dynamically initiate a step-up authentication process and lower-risk transactions will be completed seamlessly.</p>

## Conclusion

Risk Analytics is OneSpan's fraud analytics solution for online and mobile banking. This solution uses machine learning, together with an advanced rules engine and an extensive list of pre-built scenarios covering typical fraud attacks.

As such, it supports a number of different use cases out of the box, including those described in this white paper. We realize that this paper only covers a selection of use cases in which banks can leverage risk analysis. The financial world is diverse and risk analysis can be tuned to address many other applications.

We often hear from financial institutions that they already have a fraud prevention system in place. In truth, many FIs have multiple fraud solutions across retail and commercial banking. While we cannot emphasize enough how important fraud monitoring and analytics are in that battle, FIs should not consider this alone. Fraud analysis should be one of the key elements in a comprehensive, multi-layered approach to security, with a focus on line-of-sight to the mobile channel, device and app integrity, related data that the risk engine can utilize to optimize fraud accuracy, reduce false positives, etc.

At OneSpan, our mission is to help financial institutions protect their customers and their business. In thinking about your existing fraud prevention solution, it's important to understand what use cases it covers.

We can help you gain a deeper understanding of your current capabilities and limitations by discussing:

- What are your gaps or blind spots?
- How does your current system apply a continuous monitoring approach?
- How does it reduce attack propagation?
- How does it automate fraud analysts' work and boost productivity?
- How does it assess the end-points?
- How does it protect your digital banking channels?
- Is it able to leverage AI or machine learning? Is it explainable? What features is it using in the decision scoring process?

To learn more, visit our [Risk Analytics web page](#), [request a demo](#), or [contact us](#) to speak to a representative.

1. Trace Fooshee (Aite Group) at the 2019 OneSpan Investor & Analyst Day [https://s24.g4cdn.com/314592314/files/doc\\_downloads/transcript/20191204-OSPN-ID-Transcript-v2.pdf](https://s24.g4cdn.com/314592314/files/doc_downloads/transcript/20191204-OSPN-ID-Transcript-v2.pdf)
- 2, 3, 4. Aite Group, "Social Distancing: Adapting Fraud and AML Operations to COVID-19", April 2020 - <https://aitegroup.com/report/workplace-distancing-adapting-fraud-and-aml-operations-covid-19>
- 5, 6. Aite Group, "Trends in Account Takeover Fraud for 2019 and Beyond", June 2019 - <https://www.aitegroup.com/report/trends-account-takeover-fraud-2019-and-beyond>
7. Javelin Strategy & Research, "The 2020 Identity Fraud Report", May 2020 <https://www.javelinstrategy.com/press-release/identity-fraud-losses-increase-15-percent-consumer-out-pocket-costs-more-double>
8. FBI, Public Service Announcement, June 2020 - <https://www.ic3.gov/media/2020/200610.aspx>
9. Aite Group, "The Rise of Digital-First Banking", June 2020 - <https://www.aitegroup.com/report/rise-digital-first-banking>
10. American Banker, June 2020 - <https://www.americanbanker.com/news/citi-sees-surge-in-corporate-online-account-opening-amid-pandemic>
11. BankInfoSecurity, June 2020 - <https://bit.ly/3jsFlmj>
12. Kaspersky Lab, "IT threat evolution Q1 2020", May 2020 - <https://securelist.com/it-threat-evolution-q1-2020-statistics/96959>
13. Deloitte, "Accelerating Digital Transformations in Banking", September 2018 <https://bit.ly/3hFPVva>
14. Aite Group, "Mule Activity: Find the Mules and Stop the Fraud", April 2020 <https://www.aitegroup.com/report/mule-activity-find-mules-and-stop-fraud>
15. Forrester, "The State of Digital Banking, 2019", September 2019 - <https://www.forrester.com/report/The+State+Of+Digital+Banking+2019/-/E-RES157239>



OneSpan enables financial institutions and other organizations to succeed by making bold advances in their digital transformation. We do this by establishing trust in people's identities, the devices they use, and the transactions that shape their lives. We believe that this is the foundation of enhanced business enablement and growth. More than 10,000 customers, including over half of the top 100 global banks, rely on OneSpan solutions to protect their most important relationships and business processes. From digital onboarding to fraud mitigation to workflow management, OneSpan's unified, open platform reduces costs, accelerates customer acquisition, and increases customer satisfaction.



Copyright © 2020 OneSpan North America Inc., all rights reserved. OneSpan™, DIGIPASS® and CRONTO® are registered or unregistered trademarks of OneSpan North America Inc. and/or OneSpan International GmbH in the U.S. and other countries. All other trademarks or trade names are the property of their respective owners. OneSpan reserves the right to make changes to specifications at any time and without notice. The information furnished by OneSpan in this document is believed to be accurate and reliable. However, OneSpan may not be held liable for its use, nor for infringement of patents or other rights of third parties resulting from its use.  
Last Update: September 2020

To learn more, contact  
OneSpan or visit our  
[Risk Analytics web page](#)

### CONTACT US

For more information:  
[info@OneSpan.com](mailto:info@OneSpan.com)  
[www.OneSpan.com](http://www.OneSpan.com)