OneSpan
Be bold. Be secure.

BUYER'S GUIDE TO EVALUATING FRAUD DETECTION TOOLS

WHITE PAPER

TABLE OF CONTENTS

INTRODUCTION

Finding the best fraud monitoring tool for your organization can be challenging. Requirements from internal stakeholders and vendor fact sheets can give an overwhelming impression that your solution needs to "have it all and then some". In reality, your choice should simply tick all the boxes on your must-have list and cover your business use cases. It should contain most of the necessary features out-of-the-box, to minimize the need for time- and resource-consuming customizations.

What should a fraud monitoring tool include to be able to meet your needs? To start, an ideal solution should be able to identify and respond to a wide array of fraud scenarios, both industry-known and specific to your organization. However, it's also essential for the tool to be able to react to unknown and perhaps surprising fraud occurrences. It should provide a versatile mix of features to collect and analyze the data, draw correct conclusions, take actions based on results, and finally produce comprehensive reports. It should be able to integrate in your existing ecosystem and, at some point, this tool should become something your fraud team cannot imagine living without.

Clearly, that's a tall order for a fraud detection software. Not every solution on the market lives up to this standard, so it is crucial that organizations do their research and find a tool that can provide comprehensive fraud monitoring. Below, we've assembled the top nine capabilities that a fraud monitoring tool must provide in order to meet the needs of modern financial institutions.

An ideal solution should be able to identify and respond to a wide array of fraud scenarios, both industry-known and specific to your organization.

KEY FUNCTIONS OF A FRAUD MONITORING TOOL

1. Detect a Wider Range of Fraud by Combining Machine Learning with an Advanced Rule Engine

An advanced rule engine with a proper set of rules will filter out the fraudulent events meeting specific criteria. For example, the rule engine will catch transactions whose time, place or amount values deviate from a normal scenario. It can also help with detecting more sophisticated cases, like phishing attacks or transactions to mule accounts. Think about it as a system of filters that blocks transfers, allows them down the pipeline or alerts the system to step-up authentication.

But your solution should not rely solely on rules. A rule-based system can no longer keep up with fraud attacks that evolve in complexity, speed and automation. Rule libraries keep on expanding, which puts pressure on the system, slows operations and increases the false positives rate. In order to provide ultimate capabilities to combat a wide array of fraud attempts without affecting the processing speed, think of a combination of rules with machine learning algorithms.

Machine learning lives up to the hype. With the capability to analyze an incredible amount and variety of data, it is an indispensable element of your fraud detection mix. It can easily extract value from data with little human input.

Machine learning lives up to the hype. With the capability to analyze an incredible amount and variety of data, it is an indispensable element of your fraud detection mix. It can easily extract value from data with little human input.

Both supervised (learning from provided historical, labeled data) and unsupervised (learning to detect fraud without any prior labeled data input) types of machine learning are important, since they can detect different occurrences of fraud. Supervised machine learning shows its power when detecting known scenarios, whereas the unsupervised type may surprise you by finding fraudulent patterns in your customers' behavior that you have never come across before.

Choose a machine learning solution that implements different algorithms and, with support from your vendor's experts, pick the best algorithm for your situation. Look for a machine learning implementation that will provide insights into the analysis process as well as evidence about why a transaction was declined or accepted.

2. Prevent Fraud Out-of-the-box

You should expect your anti-fraud tool to be able to detect fraud right from the start. Make sure it supports your business continuity requirements and, as such, ensures a smooth transition from the existing fraud processes. You cannot afford any freeze in your anti-fraud efforts, so it's important to find a solution that will provide a sufficient level of protection out-of-the-box, from day one. A turnkey package should be available for you to analyze transactions through a combination of a rule engine and machine learning. Both should work on deployment even without reference data.

Of course, while out-of-the-box is a good start, the solution should be flexible enough to customize it to your own needs and data.

3. Apply a Dynamic Approach to Your Authentication Flows

The fraud monitoring framework should be able to integrate with existing and future multi-factor authentication options. It should constantly evaluate the risk of a particular event and, based on this evaluation, orchestrate the authentication flow. It should dynamically trigger the most suitable authentication method for a given situation, according to its risk level. For example, if a certain transaction is evaluated as suspicious, due to unusual timing, location of the user or significantly larger amount than before, your solution should be able to step up the authentication criteria instead of simply rejecting the transaction or putting it on hold for manual review.

4. Be Prepared for the Challenges Specific to the Mobile Channel and Explore the Full Potential of Data

The mobile channel brings additional challenges that distinguish it from the standard internet banking experience. Your fraud monitoring solution should recognize these distinctions. Monitoring of the mobile channel needs to take into account, among others, diversity of devices, operating systems or the fact of no control over what else is installed on these devices. Without recognizing the specifics of the mobile channel, the tool may not collect all the data points and therefore draw incorrect conclusions. Because mobile phones in general provide much richer context and enable more advanced analysis, leveraging the broader context of the mobile channel is essential for fighting mobile fraud.

Your fraud monitoring framework must provide analysis based on a wide array of data collected from your users' devices. This data can include for example device health, detecting, among others, if the device has been jailbroken or if there has been any suspicious activity. Insight can also be provided for authentication and biometrics, for example face recognition score or PIN strength. General device information is another example from a wide array of mobile-specific intelligence, and can include the version of the operating system, device model, etc.

Your fraud monitoring framework must provide analysis based on a wide array of data collected from your users' devices.

But these data points are only valuable if they are valid. This means that you should make sure that both the data collection and the transfer between the mobile device and the server are safe. A secure communication channel independent from other existing communication protocols will ensure that the device security status can be trusted upon arriving to your fraud monitoring system.

5. Continuously Analyze the Risk of the Mobile Device Across Channels and Secure all User Journeys

Bank customers expect from their omnichannel banking journey to provide a consistently high level of security and flawless user experience. Many already use mobile banking apps as the preferred channel for interacting with their banks, but a mobile device can also be used as an authentication tool for all the other channels.

Your fraud monitoring tool should support this mobile-centric omnichannel approach. By confirming that your customer's phone is secure and has not been compromised, it can help turn the phone into a trusted device used to securely authenticate its owner at ATMs, in branches, and for internet banking.

To enable the notion of a trusted device, your solution needs to operate with a broader, holistic approach that combines different elements:

- Secure data collection and storage
- Secure channel for data transfer from the mobile device
- Secure application and server-side analytics

These elements create a full and reliable picture of your customer's device with a certain risk score. The score has to be continuously assessed, and controls have to be in place to react in case the risk level increases.

6. Maximize the Efficiency of Your Fraud Team

The fraud monitoring solution will become the main tool for your fraud team's day-to-day operations. Therefore, it's not only important that it provides a wide array of controls to detect fraud. To maximize the potential of your team, consider a solution that will also provide a clear interface for alert handling and investigation with audit trail. It should have automated workflows as a built-in feature to reduce the need for manual operations. It should also utilize different types of data (hotlists, mobile device data, etc.) to provide your team with a maximum amount of relevant information.

Keep the current skillset of your analysts in mind. If you don't have a team of data scientists at your disposal, select a solution with vendor support for the machine learning algorithms. Another example can be reporting – it should be easy to access and customize.

To maximize the potential of your team, consider a solution that will also provide a clear interface for alert handling and investigation with audit trail.

7. Expect the Real-time Processing Standard

Real-time processing is an important ingredient of a good user experience model. Simply put, your users will expect a frictionless experience. They will want their transactions to be processed immediately, any time of day or night – after all, nobody likes to see an important money transfer in the pending state. From this perspective, a fraud monitoring tool should move away from batch processing (except for specific cases in corporate banking) in favor of instant feedback. Your tool should not delay the transaction. It should provide the output within milliseconds, without impacting the transaction flow.

From your analyst's perspective, the real time notion translates into a solution that enables protection at all times, with workflows that process cases within a fraction of a second. Such a solution should be able to quickly collect data and streamline it by aggregating all the collected data elements and their history into features. These features can then be used in rules or by machine learning. It should score this data and take an immediate action, all in real time and in continuous mode.

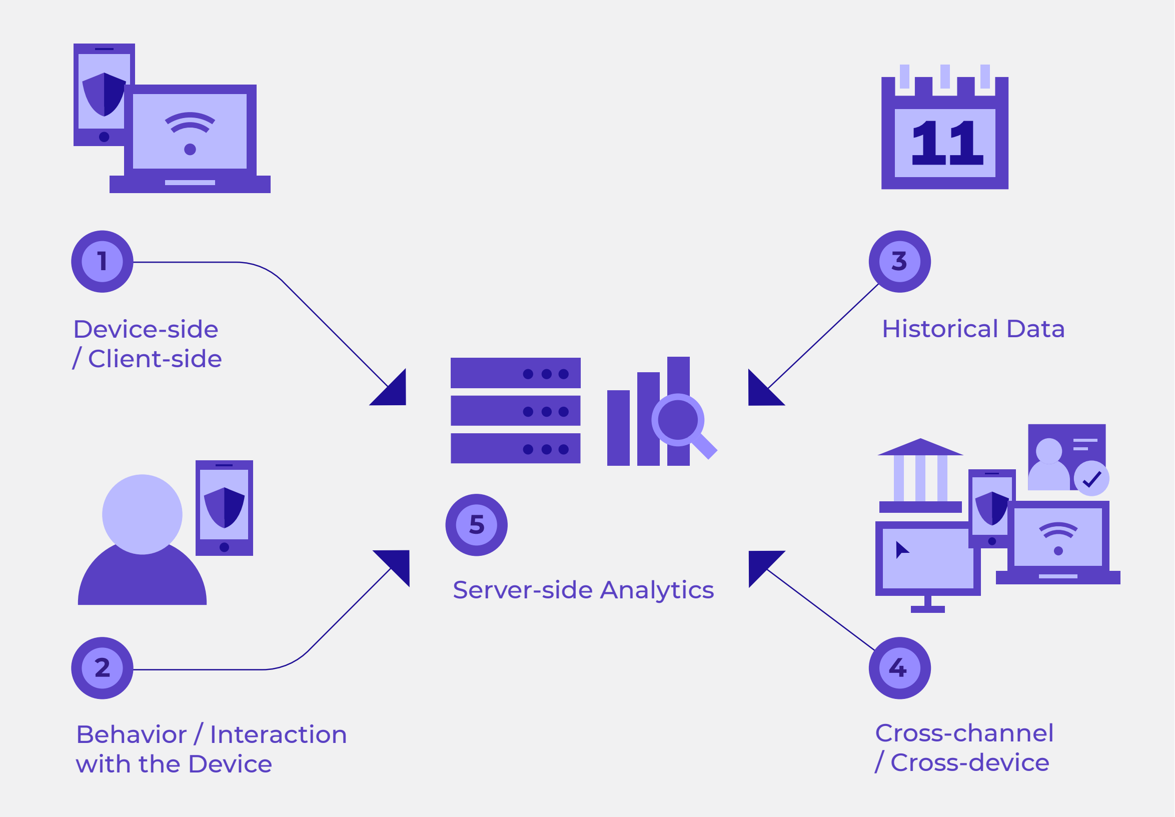
Your fraud monitoring should use this layered approach in order to create a full picture of your user and gain an understanding of their typical actions, most popular transaction times, etc.

8. Create a Layered, Context-aware Online Security Approach

We already mentioned how important it is for your anti-fraud framework to be able to collect and utilize multiple data points. This not only creates a reliable profile of the user, device and transaction, it is also essential when investigating fraud cases.

Gartner[1] emphasizes the importance of a layered security approach to protect users and accounts from fraudulent activity. As part of this approach, data should be collected and analyzed on several levels.

- **Layer 1: Device-side / Client-side** – The first layer is endpoint-centric and entails monitoring of data on a device level.
- **Layer 2: Behavior / Interaction with the Device** – The fraud monitoring tool will analyze the session navigation behavior, such as speed of browsing or accuracy of movement, to identify suspicious patterns.
- **Layer 3: Historical Data** – The third layer involves analysis of user and account activity in the particular channel on a historical basis.
- **Layer 4: Cross-channel / Cross-device** – This layer looks wider into the user behavior across channels, devices, and products.
- **Layer 5: Server-side Analytics** – Finally, the entity link-analysis layer involves server-side analytics, leveraging a decision analysis engine and machine learning.


11
1
Device-side / Client-side
3
Historical Data
5
Server-side Analytics
2
Behavior / Interaction with the Device
4
Cross-channel / Cross-device

Your fraud monitoring should use this layered approach in order to create a full picture of your user and gain an understanding of their typical actions, most popular transaction times, etc. This allows you to quickly and reliably identify and investigate any suspicious activity. Plus, if your solution can integrate with your other systems, this can create synergy and provide additional insights.

9. Ensure Compliance with Regulations (Where Applicable)

Find a fraud monitoring tool that will cover the most relevant legal requirements. Depending on laws and regulations in the countries where you do business, lack of mandatory components for compliance may be a showstopper in your buying process.

For example, when looking at the European Union's revised Payment Services Directive, you will need to meet the transaction risk monitoring expectations outlined in the relevant technical standards document. These include, among others, ability to recognize known fraud scenarios, abnormal location of the payer, abnormal spend for a user, and signs of malware infection in any session of the authentication procedure.

Fraud Detection Checklist

Ensure Your Fraud Solution:

1. Detects a wide range of fraud by combining a rules engine with machine learning
2. Provides capabilities and know-how to fight fraud from day one
3. Enables processing of events in real time
4. Answers the challenges specific to the mobile channel
5. Continuously analyzes the risk of the mobile device across channels and secures all user journeys
6. Streamlines the investigation, boosting efficiency of your fraud team
7. Applies an adaptive approach to your authentication flows, building a frictionless experience
8. Applies a layered, context-aware online security approach
9. Ensures compliance with regulations

FRAUD CONTINUES TO EVOLVE

Fraud Keeps Evolving – So Should Your Fraud Monitoring

The ultimate goal of an anti-fraud framework is to stop criminal activities while streamlining the legitimate ones. Simple tools are no longer enough. In order to efficiently identify fraud, select a solution that covers all nine aspects mentioned above, from machine learning to the ability to orchestrate the authentication flows. It may sound complex, but it should be a market standard. Fraud keeps evolving simply because it has a huge profit potential for criminals, therefore your anti-fraud weapons must evolve as well.

OneSpan has the expertise to properly secure your user journeys and enable authentication methods that dynamically adapt to risk. Contact us to learn more about our comprehensive fraud monitoring and data analytics solutions.

Fraud Detection and Prevention from OneSpan

OneSpan Risk Analytics achieves the twin goal of strong security and optimal user experience and serves as a key component of our Trusted Identity Platform. OneSpan Risk Analytics analyzes vast mobile, application, and transaction data, in real-time, to effectively detect fraud and dynamically step up security to stop fraudulent transactions, improving the customer experience and defeating sophisticated fraud.

Learn more about OneSpan Risk Analytics

[1] Paraphrased from concepts discussed in Gartner reports:
https://www.gartner.com/doc/3472117/market-guide-online-fraud-detection
https://www.gartner.com/doc/3038120/market-guide-online-fraud-detection

OneSpan

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.

CONTACT US
For more information:
info@OneSpan.com
OneSpan.com