How to Choose a Great Fraud Solution
Introduction

Never-ending data breaches, easily accessible fraud tools, and increasing volumes of sensitive online data have resulted in a constant cat and mouse game between businesses and fraudsters. As businesses try to combat evolving fraud attacks that continue to grow in complexity and sophistication, they are also addressing changing customer expectations for seamless, omnichannel experiences.

Fortunately, an effective fraud and risk management platform can actually serve as a competitive advantage, leading to increased conversion, top-line growth, reduced operational costs, higher customer loyalty, seamless customer experience, and strong brand value.

However, choosing a great fraud solution is a difficult task. Not only are there numerous fraud solutions available that differ greatly in their capabilities, but there are also problems and needs specific to each business that must be considered.

Businesses must choose from among a plethora of device, biometric, and machine learning solutions to find the best fraud solution suited for their unique challenges. And, while many solutions claim to address popular use cases, not all solutions are created equal in their ability to effectively fight fraud. Failing to provision the correct fraud management platform can lead to increased false positives, financial loss, and operational costs.

To select a great fraud solution, ensure that it is capable of the following:

• Ingests various data sources
• Flexible and scalable
• Provides proactive fraud detection
• Seamless orchestration
• Lowers operational costs
• Omnichannel view
• Low total cost of ownership
Ingests Any Data Source

Fueled by faster computing power, the growth of IoTs, and the rise of social media, data continues to grow exponentially. Businesses are now able to collect vast troves of data. However, businesses continue to struggle with how to effectively organize, use, and control big data.

Because a majority of today’s data is unstructured, businesses need a solution that goes beyond organized, structured data for a more complete view of the connecting user.

A powerful fraud prevention solution will have the ability to ingest internal and external data in any form, and then enrich it with relevant third-party data sources, such as credit bureau data, regulatory data, and phone intelligence.
Flexible and Scalable

Fraud is growing more complex, sophisticated, and is constantly evolving.

Solutions that require specialized skills to write complex statements or SQL queries in order to modify and encode them lack the flexibility needed to quickly pivot in response to changing fraud.

Businesses need a fraud solution that allows analysts to easily add, configure, modify, and optimize rules and models, as well as the ability to test the impact of those changes before they are implemented. Furthermore, as a business’ needs change and grow, the solution should have the ability to scale and adapt.
Many solutions have not kept pace with evolving fraud, which is becoming more persistent and complex. These legacy solutions have left businesses vulnerable to and ill-prepared for emerging attack patterns, which can have detrimental effects on a business’ bottom line and brand reputation.

Analyzing numerous collections of extensive data requires big data analytics and machine learning to not only detect known patterns of fraud, but also to identify new and emerging patterns that are not yet perceptible to human analysis. Furthermore, businesses need to be able to analyze data in real time in order to detect and block fraud before it escalates.

Supervised and unsupervised machine learning models that evolve based on new events and data can continuously enhance detection – giving businesses a valuable advantage in the fight against cybercrime.

Link analysis and data visualization capabilities that show the connections between data points can help fraud analysts drill down further to see how events are related.
Customer expectations are higher than ever, placing considerable pressure on businesses to quickly distinguish bad actors from legitimate customers in real time. Enabling fraudsters to slip into a business’ ecosystem can lead to significant financial loss and reputational damage. However, incorrectly insulting a legitimate customer or requiring unnecessary authentication, can lead to shopping cart abandonment, lost revenue, and defection to a competitor.

Businesses must carefully balance fraud and friction in order to create an optimal customer experience. This requires seamless, behind-the-scenes orchestration that eliminates challenges for good customers and seamlessly routes inconsistent, suspicious, and high-risk events for appropriate step-up or further review.
Improves Operational Efficiency

With fraud continuing to rise and evolve, analysts need intuitive tools to improve efficiency and productivity. An effective solution simplifies the fraud-screening process by automating previously cumbersome processes. Having a unified and intuitive user interface with the ability to easily customize workflows further boosts the productivity of fraud analysts.

Upon employing a successful fraud solution, many businesses are able to reduce manual reviews, re-allocate resources, and streamline operations.
Provides an Omnichannel View

Today’s consumers transact using a variety of devices, locations, and channels.

Fraudsters know that many businesses are still challenged when it comes to detecting fraud across multiple channels. As a result, fraudsters are not only exploiting the digital channel, but also call centers, IVR, and mobile.

Businesses need the ability to merge these various interactions from across the customer journey into a unified view to better detect suspicious behavior and events. Without an omnichannel view, critical pieces of information are missed, enabling possible fraud schemes to go undetected.
Low Total Cost of Ownership

Fraud solutions vary greatly in terms of capabilities and total cost. Many modern solutions use commodity hardware and can be deployed on a business’ existing enterprise stack. By integrating with existing systems, there is no need for businesses to purchase additional databases or other infrastructure components. This also speeds up the time it takes to implement and deploy a complete fraud solution, giving businesses immediate protection.
Conclusion

In the end, businesses need to choose a fraud solution that aligns with their unique needs and objectives. Some businesses may require a solution that is able to detect fraud across multiple payment methods, while other businesses may only be concerned with high levels of fraudulent new accounts. Whatever the specific business requirements are, having the previously discussed capabilities will result in a great fraud solution that accurately uncovers fraud and provides actionable insights – leading to faster, more effective decisioning that enhances the customer experience and positively impacts the bottom line.
ABOUT SIMILITY

Simility, a PayPal service, offers real-time risk and fraud decisioning solutions to protect global digital businesses. Simility’s offerings are underpinned by the Adaptive Decisioning Platform built with a data-first approach to deliver continuous risk assurance. By combining artificial intelligence and big-data analytics, Simility helps businesses orchestrate complex decisions to reduce friction, improve trust, and solve complex fraud problems. Built by industry veterans, Simility is trusted by some of the world’s leading consumer brands across financial services, payment processors and commerce merchants. For more information on Simility, visit Simility.com