Tip Sheet

Is the speed of fraud threatening your business?

Ever-evolving fraud schemes. Changes in regulatory requirements. New digital initiatives. Increasing expectations for an enhanced customer experience. Keeping up with these shifting dynamics is a constant struggle for fraud and compliance teams.

These fluctuating conditions have negatively impacted businesses' ability to fight fraud. Systems have become increasingly complex, expensive, and difficult to integrate and manage. This complexity limits your ability to quickly scale and adjust in response to new risks and causes too much friction for customers.

How extensive is this impact? There's currently a 35 percent year-over-year increase in mobile commerce. And one in 10 new applicants is likely to be an imposter using breached data. New fraud schemes are developing daily, and yet $40 billion of legitimate customer sales are declined annually because of tight rules and processes causing false declines. On top of that, fraudsters aren't the only ones evolving. Financial institutions also have to raise the bar to meet consumer expectations.

This rapidly shifting environment only reinforces the need for aggressive fraud prevention strategies and adoption of new technologies to prepare for the latest emerging cybersecurity threats — all while continuing to protect all parties' interests. Fraudsters have what they need to be quick and flexible. Why shouldn't businesses?

Fraud prevention teams need a faster, easier way to maximize their existing systems and to deploy new products. They want to be as nimble and agile as fraudsters. Future-proofing your fraud prevention strategy is the best path forward. Teams can protect the customer experience while still minimizing fraud and compliance risk. Here are two keys to successfully and strategically future-proofing your fraud prevention:

Future-proofing

Position your organization for success in this ever-changing landscape. It's the best way to manage fraud and identity services.

Tip sheet

Is the speed of fraud threatening your business?

1. An open approach

Switching from one solution to another as your authentication needs change takes time. And time is costly — especially when customer expectations are so high. By managing disparate systems from one source, businesses can increase operational efficiency by avoiding needless referrals and drive down the cost to deploy new tools. Additionally, this supports a layered approach to managing risk across all providers and reduces the expense of managing multiple services over time.

Fraud prevention experts agree. Since there's no silver bullet to stop fraud, businesses need to apply a layered approach that can be orchestrated like a fine-tuned symphony. Only when you weave your disparate systems together and direct their workflows from one source can you compete with the multitude of fraudsters on the attack.

Stopping fraud at all costs isn't realistic. Businesses have financial targets to meet. So, a strong bottom line is often built on tough choices. At what price point does fraudulent activity outweigh fraud prevention? Stopping fraud must be operationally efficient to ensure your efforts don't cost more than the fraud itself. With an open approach, fraud teams benefit from single sign-on access to multiple systems — and the scale and flexibility to increase the time to market for new and enhanced strategies and services. A common application program interface (API) allows for reduced integration costs and complexity and, in turn, drives top-line growth by reducing friction and false positives that cause customer fallout.

2. Hands-on workflow decisioning

Thirty percent of online customers are interrupted to catch just one fraudulent attempt. Outdated fraud strategies can cost your organization millions. Fraud teams can't wait on technical resources to alter strategies and address new fraud patterns and attacks. To keep up with agile criminals, teams need direct control so they can quickly select and order the appropriate services and decision criteria for each transaction. Fraud teams require the ability to call services all at once or in sequence based on decision logic and precisely tailor strategies based on transaction type.

With hands-on workflow decisioning, fraud prevention teams have what they need at their fingertips. They're positioned to optimize decisions across services, control the data used, and apply client-specific data and analytics. With fraud and identity solutions working together under the direction of fraud prevention experts, your business can reduce friction and false positives.

There are many challenges with legacy systems that make it difficult to scale and adapt in response to business opportunities and fraud threats. Rather than replacing these systems, businesses need to manage them as one layered defensive line.

Future-proof your fraud strategies with an open approach and hands-on workflow decisioning capabilities. It's the only way to keep pace with the speed of fraud.

Let's get started

Experian
475 Anton Blvd.
Costa Mesa, CA 92626
T: 1 888 727 8330
www.experian.com

08/17 • 2000/1280• 1112-DA