Tip sheet

Fraud's evolving...but so are you

Three trends that will help you outsmart fraudsters

Introduction

Fraud loss has long been accepted as a cost of doing business. But something has changed. Fraudsters have evolved—they leverage technology and sophisticated underground networks—and actual losses now exceed expected losses. To plug the holes and patch the gaps, fraud prevention has become overly complex and is negatively impacting the customer experience.

Fraudsters are relentless. They count on vulnerabilities that you can eliminate. They expect to be chased, not outmaneuvered. Organizations need to be as forward-looking in fighting fraud as they are in growing revenue and attracting new customers. It's time to move beyond one-size-fits-all fraud strategies and instead deploy right-sized solutions so that the appropriate level of protection is applied to every single transaction for increased confidence and effortless customer interactions.

The reality of today's economy demands this change. Business is global—it happens 24 hours a day across countless digital and face-to-face settings. Creating a secure, streamlined customer experience is paramount. Although once considered separate mandates managed by separate teams, revenue generation and fraud prevention are now intrinsically linked. Siloed ways of working are no longer viable. In fact, the more closely aligned your product development, marketing, customer experience, and fraud risk strategies are, the more successful your business will be.

Modern fraud mitigation approaches make it possible for fraud prevention to play an active role in driving growth and a positive customer experience. Here are three industry trends that can help modernize your fraud mitigation strategies:

1. Machine learning

Machine learning has become an invaluable tool in the fight against fraud. It combines computational statistics, artificial intelligence, signal processing, optimization, and other methods to identify patterns. Machine learning has been a significant breakthrough in helping companies move from reactive to predictive by highlighting suspicious attributes or relationships that may be invisible to the naked eye but indicate a larger pattern of fraud.

Traditionally, supervised learning has strictly been used by the majority of machine learning systems. Supervised learning applies prior knowledge of fraud tactics to guide pattern identification. This learning is easy to teach the machine once there is a clear target. The system, while valuable, has some limitations, including the extensive time it takes to react and prevent fraud. Additionally, the poor use of machine learning can generate a lot of false positives. One way to increase the accuracy of supervised machine learning-based fraud detection is to pair it with unsupervised machine learning techniques that look for irregular or uncharacteristic items.

2. Anomaly detection

Unsupervised machine learning techniques, also known as anomaly detection models, complement supervised learning by looking for aberrations in the patterns of a transaction flow. These deviations may indicate fraud, or may simply be a change in global behavior (or what "normal" behavior looks like). For this reason, anomaly detection models are a strong complement to supervised learning approaches because they manage the same problem from entirely different angles and exploit orthogonal information. When combining both techniques, the resulting analytic engine can recognize previous patterns of confirmed fraud, while also raising an alert if a pattern of activity changes. While making both techniques work together requires robust machine learning expertise, the combined approach provides optimal performance—increasing fraud detection rates and reducing false positives.

3. Hybrid approach: Machine-based learning and characteristic-based analytics

Fraud experts are deeply immersed in studying fraud behavior—including understanding the psychology of different types of criminals. They also have years of hands-on experience working in the fraud prevention field—and often in multiple industries. These fraud experts bring the insights needed to both guide machine learning and create characteristic-based analytics. Characteristic-based (or rules-based) analytics combines this highly specialized expertise with machine learning—which we call a hybrid approach.

By combining machine and human intelligence, organizations are able to significantly reduce the number of false positives (reducing friction on legitimate customers) and enhance predictive fraud detection (to mitigate fraud losses and brand damage).

Modern fraud mitigation approaches have shifted fraud prevention from "the cost of doing business" to an important driver on the growth agenda with an active role in a company's success. To outpace fraudsters, you must modernize your fraud mitigation strategies, making them less reactive, and more proactive.

Ready to fight fraud while providing a first-rate experience that inspires customer loyalty? We're here to help.

Let's get started

Experian
475 Anton Blvd.
Costa Mesa, CA 92626

T: 1 888 727 8330
www.experian.com

8/17 • 2000/1274 • 1106-DA