Tip sheet

How to modernize fraud prevention in five steps

Introduction

Fraudsters are determined and relentless. With constantly evolving schemes and alternative methods, fraud prevention has become more difficult than ever. Factor in economic conditions, regulatory requirements and resource limitations and you might feel like it's impossible to keep pace.

So, how can you stay a step ahead? These five strategies can help you outmaneuver fraudsters—decreasing risk while ensuring the positive experience your customers deserve:

1. Apply right-sized fraud solutions to reduce unnecessary customer disruption and manage risk

Fraudsters hide in plain sight, blending in with legitimate customer traffic—which is why companies accept a certain amount of customer disruption as an undesirable but necessary part of catching fraudsters. The level of this disruption is wildly out of balance, however. The ratio of disrupted legitimate traffic to actual fraud attempts is now as high as 30 to 1. In other words, 30 legitimate customers are challenged or blocked—for reasons they rarely understand—to catch one fraudster. As more purchases move to the online channel, this rate will only increase. The net result is a consumer population irritated by the unending number of challenges to their online activity, as opposed to just a few years ago when consumers welcomed banks and finance companies protecting customers from the "bad guys."

To reduce customer disruption and appropriately manage fraud risk, companies need to apply fraud mitigation strategies that reflect the value and level of confidence needed for each transaction. We call this right-sizing the fraud solution. For example, if actual fraud attacks represent 1 to 2 percent of transactions, right-sized solutions should identify no more than 4 to 6 percent of transactions as probable fraud. This approach, when aligned with your company's fraud rates and commercial strategy, increases the likelihood of catching fraudsters without disrupting the business of (and relationships with) legitimate customers.

2. Get a universal view of the consumer

Companies try to reduce the anonymity of the online world by verifying customers primarily through identity challenge techniques (i.e., challenge-response questions), but the harsh reality is that most identity data has been compromised. In the past two years alone, more than 2.2 billion personal records have been exposed as the result of data breaches[1]. According to Javelin, one in five data breach victims

suffered fraud in 2015, a rise from one in seven in 2014[2]. A multi-layered approach to authentication is considered the gold standard for identifying legitimate customers, but this can be hard to do without creating so many challenges that the customer experience is adversely affected. Knowing the individual customer extends beyond a traditional 360-degree view. It means having knowledge of a person's offline and online behavior, not only with your business, but with others. This information requires a more expansive view and collaboration across teams within a company, businesses within an industry, and across different industries. Applying the insights from information such as online behavior, historical transactions, identity, biometrics, and device intelligence gives companies a more expansive view. It means truly being able to know and recognize your customer, and making their interactions with your business relevant every time.

Having access and insight into this universal consumer behavior, down to the transaction level, will be necessary for fraud mitigation in the future. The ability to know and recognize a legitimate customer will make fraudsters easier to differentiate. This will mean fewer unnecessary and aggravating challenges to customers—frictionless is the future. It will also help achieve higher conversion rates for marketing campaigns and improve marketing return on investment by delivering the right message to the right person when they are most receptive to it and in the most convenient channel. Taken together, this is a clear example of the benefits of converging mandates around business growth and fraud mitigation.

3. Expand your customer view through a blended ecosystem

Many organizations have launched projects to achieve a single customer view: collaborating across internal silos to bring together information about their customers and their interactions. While they're good in theory, the conflicting priorities of internal silos turn these projects into multi-year undertakings that are challenging and costly. Even if attained, a company's single-customer view may still achieve only a partial view of the consumer.

This is because their view is solely based on their relationship, rather than the consumer's relationships with other companies. Fraudsters on the other hand have this broader view, and they use it to their advantage

The volume of compromised data and ever-changing fraud schemes has created a threat landscape that can no longer be managed in a siloed manner. Increasingly, companies are participating in a blended ecosystem—working with vendors, customers, partners and even competitors—that can bridge disparate data and internal siloes. The result is an enhanced customer experience that supports business growth, without sacrificing protection.

4. Become agile and scalable using service-based models

Fraudsters act fast, and companies must at least keep pace (and preferably be a step ahead). To spot the latest fraud attacks, many large institutions employ statisticians and modelers to monitor and develop rules based on different combinations of variables. These complex fraud risk models require a lot of time and investment to set up and maintain and, therefore, a significant business case is needed to gain approval to proceed. Once approved, it takes time – often months – to analyze, build and deploy the models. It's only at that point that companies can respond to the threat, but by then it's likely that fraudsters have done damage.

Fraud adapts quickly, and when you're too slow to respond to threats, it can come at great expense to your business and customers. Your systems and business processes become a source of vulnerability—which is why more companies are turning to service-based models that provide greater agility and faster response to emerging threats. Service-based fraud models give you the benefit of highly skilled expert analysis. An analysis that is regularly updated to respond to fraud trends or incidents seen across the industry at any given time, often protecting you before the fraud happens. These service-based fraud models also adapt and scale to support your business, no matter how fast your volume grows or which products, channels or geographies you pursue.

5. Future-proof your solution

Companies need to be as nimble as fraudsters, with fast access to the right tools and data whenever they need it. But that's often not the case, leaving companies in the wake of evolving fraud schemes. The current approach of adding new tools on top of existing solutions is creating complexity that is becoming expensive to integrate and difficult to manage. You need flexibility and scale, to get more out of what you have in place, test strategies and utilize new technology. You need a way to connect the best solutions available and access a range of data sources to keep up with the speed of fraud.

These strategies can change the dynamics between companies and fraudsters. The internal collaboration it requires can offer many ongoing benefits, including having a broader customer view and ensuring everyone supports the same end goals. Importantly, it also means customers encounter fewer points of friction with strategies that are put in place to protect them—so you provide the best experience to your valuable clients.

Are you modernizing your fraud prevention strategy?
Let us help you get started.

Contact us

1 Experian data on file

2 Javelin 2016 Identity Fraud: Fraud Hits and Inflection Point, February 2016

Experian
475 Anton Blvd.
Costa Mesa, CA 92626

T: 1 888 727 8330
www.experian.com

7/17 • 2000/1273 • 1105-DA