JUNE 20 • 2017 ONLINE EDITION

Forbes

TECHNOLOGY

Fraud Prevention:
Get Ready Before It's Too Late

BY FORBES TECHNOLOGY COUNCIL

POST WRITTEN BY
RICARDO VILLADIEGO
CONTRIBUTOR
Founder and CEO of Easy Solutions, a Cyxtera Business, which is a global leader in electronic fraud protection.

As online transactions continue to increase and consumers become ever more dependent on online purchases, the number of threats jeopardizing these transactions grows. Every online customer action has the potential to create a reaction from a fraudster.

How bad is the fraud issue?

According to PYMNTS.com's Global Fraud Attack Index, online fraud attacks increased by 11% between the first quarter of 2015 and the first quarter of 2016. The attack rate against digital goods more than quadrupled, and it almost doubled for luxury goods. As of 2016, for every $100 in online sales, $4.79 is at risk; that's up from $1.89 in the first quarter of 2015.

What's The Current Situation?

All too often, organizations take on fraud protection on a case-by-case basis, not taking action until a crisis occurs and then, once the issue has passed, resuming normal operations. By employing this type of strategy, these organizations fail to fix vulnerabilities, leaving themselves at a much higher risk of future attacks.

Unfortunately, the consequences of this lack of protection go beyond the risk and hassle of having to constantly fight attacks. Incremental expenses are constantly added to a company's bottom line as IT manually completes anti-fraud processes with a high risk of false positives. Customers' trust and the quality of their experiences slowly erodes, putting them at risk for making the decision to take their business to a company with a better-functioning online platform.

Why Aren't Financial Institutions More Proactive In Their Fraud Protection?

A continuously recurring problem is the erroneous belief that picking one best-of-breed solution solves the entire fraud prevention problem. This is often seen when different departments are tasked with handling different aspects of fraud prevention. When this occurs, it becomes difficult to understand who is dealing with which aspect of a fraud problem.

Banks have been dealing with various types of fraud for years and have developed some ad hoc deployments that are simply not as effective as they promise to be. Fraudsters are relentless when trying to find workarounds to existing anti-fraud systems, which can quickly become obsolete. The types of systems that are frequently implemented after a crisis has occurred are usually not well thought out. As a result, they are more easily exploited when fraudsters return to attack again.

A 2016 report by Gartner (paywall) noted that "by 2021, 60% of enterprise e-commerce retailers will fast-track an integration to a new fraud prevention technology during or following a fraud attack without adequate analysis, leaving data and operational gaps, excessive false positives, preventable fraud and operational inefficiencies."

In short, quicker isn't always better when it comes to implementing anti-fraud protections. Instead of putting a Band-Aid on a bullet hole, it's important to have an effective, comprehensive solution.

Seven Tips To Help Decrease Your Risk Of Fraud

1. It is essential to ask the right questions before jumping into a technology solution. Some of these include:

- What are your greatest risks based on cyberthreats, economic climate, previous threats, business growth and geographic risks? Make sure risks are assessed based on facts, not assumptions, and that your solution addresses the unique fraud challenges of your organization.

- If an incident has already occurred, when and where did the transactions occur? Looking into these transaction activities over a period of time can help identify dips and spikes in vulnerabilities.

- Out of all your business processes, which ones have the highest risk of fraud?

2. Take on a more proactive mindset regarding fraud prevention. Be sure to consider the entire problem and not just pieces of it. Use this information to create a multilayered approach to resolving issues.

3. Employ an inclusive monitoring service that works outside the perimeter of your organization as part of this proactive approach. This monitoring service must detect and remove threats before end users realize there is a problem.

4. Understand that there is no single solution that can stop every kind of attack. Cybercriminals will exploit multiple channels, often at once, and frequently purchase tools to help them defeat anti-fraud protections. A multilayered approach is necessary to defeat ever-evolving fraud attacks.

5. Use structured and unstructured data to your advantage. While it may be tempting to focus on structured databases found in your transactional systems, it's important to move beyond descriptive analytics and look at forms of unstructured data such as social media, email and more.

6. Always remember the importance of communication among the anti-fraud team, as well as within management. It's important to build a multidisciplinary team that includes not only data scientists but also stakeholders, IT staff and business users. You need to communicate across these different departments while also keeping stakeholders up to date.

7. Keep an anti-fraud schedule. When creating a proactive plan for fraud prevention, it's essential to create a realistic timetable. Properly deploying fraud prevention across the enterprise takes time, and jumping into a quick solution can often lead to mistakes.

Changing Your Fraud Prevention Mindset

By now, it should be clear to business leaders that proactive protection is more important than ever before. A well-planned anti-fraud design is the foundation upon which future business success is built, especially during the continuing years of the digital revolution where literally every digital interaction could be at risk.

Your company executives need to keep the future of the organization in mind and approve the time and money that is required to develop a comprehensive fraud prevention plan. It is in everyone's best interest to understand that fraud prevention is not a one-and-done expense but an ongoing process that will need to evolve as new threats develop. Without a strong, proactive anti-fraud strategy to protect you against the clear and present danger of cyberattacks, the next big fraud incident that makes headlines across the world could be the one that causes irreparable damage to your brand.

Forbes Technology Council
Forbes Technology Council is an invitation-only organization comprised of elite CIOs, CTOs and technology executives. Members are hand-selected by the Council's selection committee. Find out if you qualify at forbestechcouncil.com/qualify