ECOMMERCE FRAUD TRENDS 2020

13 leading eCommerce fraud prevention solutions tell you the threats you need to prepare for in the coming year.

www.merchantfraudjournal.com

Fraud.net

Fraud.net operates a real-time fraud detection and analytics platform, helping enterprises quickly identify transactional anomalies and pinpoint fraud using big data and live-streaming visualizations. The platform allows organizations to monitor their fraud program's performance, identify process improvements, and gain insights into developing fraud trends in minutes instead of months.

www.fraud.net

What are the technological trends in 2020 that will help merchants deal with increasingly sophisticated fraud attacks?

Fraud is more nuanced, more complex and evolving faster than ever before. Perpetrators are armed with increasingly powerful computing, detailed consumer data, advanced algorithms, and more capital. These groups can successfully iterate their way to defrauding even our most revered companies, circumventing even the most advanced defenses from this past decade.

For years, it was enough for a large organization to look only inward for the data needed to build their risk management program. Some companies would share blacklists of single-dimensional metrics (names, addresses, emails and phone numbers), usually with some degree of success. Today, however, fraudsters' ability to purchase or manipulate identity elements renders both strategies relatively ineffective.

Data Enrichment

Credit agencies and identity assurance companies that can help mitigate risks of identity theft and more traditional fraud types. If industry regulators don't already require you to build a comprehensive profile on your customers, you will likely find a bank-level 'know your customer' analysis to be an invaluable tool both in containing application fraud and in growing your business. Biometric-based identity vendors are also able to address more specialized needs for identity verification. To help capture contextual variables, there are also data vendors specializing in everything from social media to the dark web, many of which should be evaluated and whose ROIs can be easily measured.

Consortium & Collaborative Data

Above all, collaborate. Fraud.net operates a modern consortium, which includes over 2,000 features and attributes to enable the hundreds of participating enterprises to identify and prevent fraud on its first attempt. We have seen and 'fingerprinted' over 600 unique fraud methods in the past year alone. For those not in a network, it would be economically infeasible to identify these on their own as it would involve being hit each type of fraud.

Platforms & Unification of Silos

Risk departments at large organizations operate by necessity in a rules-based framework. For decades, this has been the most efficient means of segmenting and managing customers and transactions. Over time, however, the logic behind these rules become outdated and then those same rules create rigidity. As rules become more numerous and rulesets become more complex, it becomes much more difficult to understand the rules' interconnectedness, to measure their effectiveness, and to make changes without creating unintended consequences.

Agility is king in the new era of fraud prevention. Platforms are where it all comes together, enabling enterprises to organize and consolidate their siloed data. Data is then appended from a myriad of 3rd party providers, and machine learning and artificial intelligence models are applied. This makes it actionable and available to improve decision-making at every level of the organization.

How do you see the implementation and enforcement of PSD2 impacting the way international merchants doing business in Europe will think about fraud prevention?

The implementation and enforcement of PSD2 represents a significant step forward in the world of payments. Consumers will benefit from more transparency and lower fees. Merchants will benefit from extra revenues and better control over the user experience. One of the more hotly debated requirements of PSD2, however, revolves around Strong Customer Authentication (SCA). Any merchant familiar with 3-D Secure, one method of authenticating users during a credit card purchase, are also familiar with the customer friction that these extra measures can cause, unintentionally resulting in the loss of legitimate sales.

While the specific SCA requirement has been delayed largely to address this issue, designed properly, a multi-factor authentication process can be initiated on confirmation of the transaction without any downside risk. It is widely agreed that multi-factor authentication does effectively reduce certain types of fraud, such as account takeover. International merchants doing business in the EU will likely warm up to the process and ultimately apply some of these best practices in other parts of the world.

What is the biggest 2020 trend that you preparing for that you believe people aren't talking about enough right now?

With these highly sophisticated tools in the hands of highly motivated and organized rings of fraudsters, we have seen dramatic increases in a few specific fraud types. By mitigating the following risks, you will be ahead in 2020.

AI-enabled Account Takeover: Most commonly, the attackers will deploy an army of bots with credentials that have been purchased on the dark web or acquired directly in a data breach. The data can be further enriched from the individual victims using a wide variety of social engineering. The sheer size of these attacks will quickly expose which merchants and financial institutions have not taken proper precautions.

Synthetic Identity Fraud: Fraudsters are able to create fabricated identities using legitimate seed data like a social security number, leaving banks and digital merchants especially vulnerable. If you don't catch synthetic identity accounts early, they can be very difficult to catch because they exhibit all the behaviors of an ideal customer. Even companies as agile as Facebook and Google were caught flat-footed and defrauded for more than $140 million this year.

Vendor and Payroll Fraud: Corporate victims of payroll, vendor and invoice fraud are almost always targeted in advance. Fraudsters study the companies' business models, supply chain, new initiatives, and contact information for the companies' personnel. Often, the attack will be preceded by a spike in spoofed emails sent to companies' human resources or payroll departments.

Insider Fraud: If cybersecurity efforts keeps fraudsters from accessing a company's data directly, they can resort to recruiting disgruntled employees or look to exploit the negligence of other personnel. Fraudsters sometimes have gained access to employees and the company's networks for years in advance without detection. Seeking financial, identity, trade secrets and other proprietary data, their motives are usually financial.

There are over 600 distinct fraud methods, each has its own characteristics and manifests with a specific set of symptoms. But, rest assured, we are focused on and prepared to detect and prevent these new threats in 2020 and beyond.

Whitney Anderson
CEO, Fraud.net

Whitney Anderson, CEO of Fraud.net, is a serial entrepreneur with over 25 years of experience in technology, digital commerce, applied AI/machine learning, and problem-solving. He is passionate about building fast-growth companies and driving game-changing value for large organizations. Former CEO of MotherNature.com - on of Inc 500|5000 fastest growing US merchants. Prior, he held executive positions at Kroll Associates and Bank of America. Whitney is a graduate of Cornell University.