????????

????????

???Sanjay Bhakta ? Muthukaruppan Lakshmanan



E-commerce shows no signs of slowing down. According to eMarketer, global e-commerce sales will grow from $3.351 trillion in 2019 to $6.169 trillion in 2023, thanks in part to the dramatic shift to online retail that happened in 2020. But there is a downside to that growth: a surge in online fraud. With more people going online to visit retailers' sites and buy from them, fraudsters are stepping up their attempts to cheat and steal.

According to Worldpay's 2021 Payment and Risk Mitigation Survey of merchants, payment fraud affects 60 percent of merchants' direct costs including revenue losses, higher chargeback volume, back-office operational expenses, and legal fees. In addition, fraud hurts the entire ecosystem, including the e-commerce and mobile commerce companies that work with retailers. And it's not just that there is more fraud -- fraudsters are also getting more sophisticated about the tools they use, ranging from identity theft to account takeovers. In fact, fraudulent activity can disrupt the entire customer journey, from awareness to post-purchase.

What makes the situation even more complicated is that retailers are operating in an increasingly complex network of information technology systems connected to multiple parties. Fraud use cases, sources of truth, and processing occurs in various systems and parties, which adds to the complexity of dealing with fraud.

These factors make fraud management an increasingly difficult process to manage by in-house information technology teams. Worldpay says, “A recurring theme in the results of our survey were the difficulties businesses experienced managing payments in-house. The complexity of managing multiple payment solutions, keeping pace with new payment methods and rising consumer expectations, managing multiple payment partners and the lack of internal payment expertise are challenges that weigh heavily on today’s merchants.”

Retailers are paying a steep price. According to LexisNexis Risk Solutions, every $1 of fraud now costs U.S. retail and eCommerce merchants $3.60 which is 15 percent higher than the pre-Covid study in 2019 which was at $3.13. This also represents a 7.1 percent rise since the 2020 survey which was conducted during the pandemic.

Retailers need a better way to rapidly anticipate and respond to increasingly sophisticated forms of fraud. On the one hand, retailers need artificial intelligence (AI) that make it possible for fraud detection to deploy machine learning in order to anticipate and newer forms of constantly evolving fraud and to outthink the criminals. But AI-fueled technology is only as good as the data used to train it to learn. Retailers also need access to industry expertise and best practices that human beings provide in partnership with technology.

This combination of AI and human expertise is known as augmented intelligence. Gartner defines augmented intelligence as a human-centered partnership model of people and artificial intelligence (AI) working together to enhance cognitive performance, including learning, decision making and new experiences.

Centific has developed an augmented intelligence framework that encompasses people, process, and platform pillars to operationalize anti-fraud efforts at scale. This approach accelerates efficiencies, while delivering value through agility. Our recently published white paper, *Fighting Online Retail Fraud with Augmented Intelligence*, contains more insight into the fraud problem and our approach. Download the white paper to learn more about how we've applied our approach to successfully fight online retail fraud.

-
-
-
-