[?????????]

?????????

???Peter Schultz



Fighting retail fraud online will require more collaboration between card processors and merchants. That was a major takeaway from Sarah Strauss of Capital One, who discussed the future of payments from an issuer's perspective at the annual Merchant Risk Council (MRC) Vegas 2022 event recently.

About MRC 2022

MRC 2022, which happened March 7-10, brought together leaders in the eCommerce payments and fraud prevention ecosystem. And they had a lot to talk about. 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. At MRC 2022, businesses ranging from Microsoft to PayPal convened to discuss the state of the industry.

Capital One Discusses Challenges from an Issuer's Perspective

In her keynote, Sarah Strauss, senior vice president, head of Fraud & Customer Servicing Strategy at Capital One, offered insight into some of the challenges that card issuers face with fraud. Her main message to merchants: we're in the same boat you are, and we experience pain, too.

For context: the processor's perspective on fraud has not always been top of mind for merchants. The widespread perception in retail is that merchants bear the brunt of the pain resulting from card fraud. If someone defrauds a merchant using someone else's credit card, the merchant has had to pay a price not once but twice: they've lost money on the value of the product stolen, and they've also been required to compensate the legitimate card owner whose card was stolen.

This problem has been getting worse with the rise of eCommerce. With an eCommerce purchase, someone can defraud a merchant using information from a card even if the fraudster lacks access to the physical card. That's why Card Not Present purchases (i.e., no physical card is used to make the purchase) are a huge area of concern and a reason why return fraud costs retailers $23 billion in 2021. It's harder for a merchant to stop this kind of fraud because the merchant has no way of confirming the purchaser's identity.

Sarah Strauss reminded everyone at the conference that the card processor pays when fraud happens, too. When a customer notices on their statement a purchase they do not recognize, the first thing they do is call their processor. From there, the processor needs to:

- Assure the customer they are taking action.
- Put in a claim with the merchant.
- Refund the customer pending resolution of the claim.
- Follow up on the claim.

Any number of things might happen during the above chain of events:

- The retailer may compensate the issuer if indeed fraud has happened.
- The retailer might dispute the customer's claim. For instance, the purchase might be legitimate, and the customer simply forgot making it.

Even if the follow-through happens perfectly, the issuer needs to pay for the administrative costs. And if a hitch arises – say, if the merchant disputes the fraud – then the issuer may suffer a customer service issue (the card holder blames the issuer because the problem wasn't fixed right away).

So, what is the solution? Sarah Strauss pointed to the use of better identity validation online, such as technology that makes it possible for a merchant to require a purchaser to upload some form of personal identification with Card Not Present purchases. But even that approach is not perfect. Driver's licenses can get stolen and used for fraud, and with state governments renewing them by mail, the risk increases.

Integration with data providers is another answer. In fact, Capital One announced during MRC an integration between Capital One's Enhanced Decisioning Data product and Forter Trusted Authorization, one of the industry's first solutions that enables merchants to have a direct connection with issuing banks to share Forter's fraud insights to increase authorization rates and decrease false declines.

At Centific, we agree that fighting fraud is no single company's responsibility. The problem requires a concerted effort from all players in the ecosystem. we recommend that retailers:

- Consider return fraud in context of a broader strategy to fight fraud. Understand the big picture and how forms of fraud relate to each other.
- Bolster your intelligence with people. Many businesses think of fraud as a technology problem, but the solution needs to start with humans in the loop. Fraud team first needs people with deep expertise in prevention, detection, and resolution. That base of human expertise needs to operate 24/7 to search for and mitigate against fraudulent transaction activity for the safety of your customers and their customers. Yes, AI-enabled technology is necessary (no human can fight fraud without AI). But AI must support a human intelligence team. People, empowered with the cognitive decisioning platform, must analyze and assess the customer journey in an e-commerce transaction, from identity verification through purchasing. People are also needed to train AI models to catch fraud and to avoid mistakes such as flagging valid transactions as fraudulent.

Doing this requires retailers to combine better tools, best practices, and partnerships to reduce risk, improve the customer experience, and safeguard the business.

That's what we do at Centific. Centific's fraud protection service and solution has reduced risk through accelerated detection, classification, protection, and real-time monitoring using the cognitive decisioning platform in a robust way, further augmented by our human intelligence team of experts around the globe. Our AI fraud protection framework has realized business value as demonstrated by reductions of false positives by 20 percent; more than $100 million in operating expense savings; and an increase in revenue of more than 10 percent with improved bank acceptance rate of transactions.

Contact Centific

Online return fraud is getting worse. But retailers can beat the criminals by combining AI with human oversight and processes. To learn more about how we can help you fight fraud with augmented intelligence, contact Centific.

-
-
-
-
-