Crafting a multi-faceted fraud prevention strategy

Lucy Hubbard

As fraudsters find new ways to commit credit card fraud, it is important that credit departments take on layered approach to protect their company from major losses.

Why it matters: In recent years, credit card fraud has loomed larger in the business credit community, with the popularization of e-commerce business environments and the rapid development of artificial intelligence, there are more and more areas where companies may be vulnerable.

The best defense against credit card fraud is to learn the warning signs so that the transaction can be stopped at the onset, rather than trying to reduce losses retroactively. There is no single indicator that will always determine if a transaction is fraudulent, but a series of inconsistencies or anomalies that should catch credit manager's attention.

"Look out for mismatched billing and shipping addresses, repeated transaction attempts in rapid succession and the use of multiple cards for one order," said Mark Tapia, vice president of business development for United TranzActions (Miramar, FL). "If a customer's order looks unusual, maybe deviating from their standard purchase, that can also be a red flag. There's no single red flag that points to fraud. There are multiple areas you should pay attention to and make note of sequences of anomalies."

Another common thread among fraud tactics is a sense of pressure, with the supposed customer stressing the urgent need for materials. "The sense of urgency is one of things we look for in fraud," said Leila Wolfe, CBF, credit manager at Ferguson Enterprises (Nashville, TN). "They give you the sense that the transaction needs to be done right now, which is when you pause and say, 'I'm going to have to call you right because I'm going to call back the person I know and see if this is actually a legitimate purchase.'"

When addressing a matter as complicated as credit card fraud, there is no single step that will protect your company, rather a series of protective measures. "Companies should implement a layered fraud strategy," Tapia said. "Using Address Verification Services (AVS) and CVV validation to ensure when processing transactions without a card that the information provided is correct. Velocity controls, that put limits on transaction amounts and frequency."

Credit managers can also consider tokenization, the act of replacing a customer's credit card number with a meaningless token, to protect customer's payment details. "Instead of storing a credit card number in your system for future payments, you can replace that card with a token provided by your service provider," Tapia said. "Then you don't have to worry about anyone ever being able to intercept the card number. It's important to add preventative measures to protect sensitive data stored within your company."

While your credit procedures could be airtight, seemingly accounting for any trick a fraudster may pull, they must be continuously reevaluated and updated to account for the rapidly evolving business environment.

"Processes should be reviewed at least annually," Kelly said. "Not only is fraud getting more advanced, but regulatory laws change. We have to think like the fraudsters to figure out how to outsmart them. People will find a way to steal and commit fraud if they try hard enough, we just have to be ahead of that

the best we can and we have to trust our business partners. We have to stay on top of education, and be aware that you have to educate the people accepting these cards and teach them to signs to look for. It doesn't do any good if a manager is taking all these classes if they are not taking the time to train their people."

The bottom line: As credit card fraud becomes increasingly harder to spot with more and more business being done in digital spaces, it is important that credit managers build fraud protection into their credit processes and commit to continuously reevaluating and building onto procedures as fraud evolves.