Fine-tuning Fraud Protection

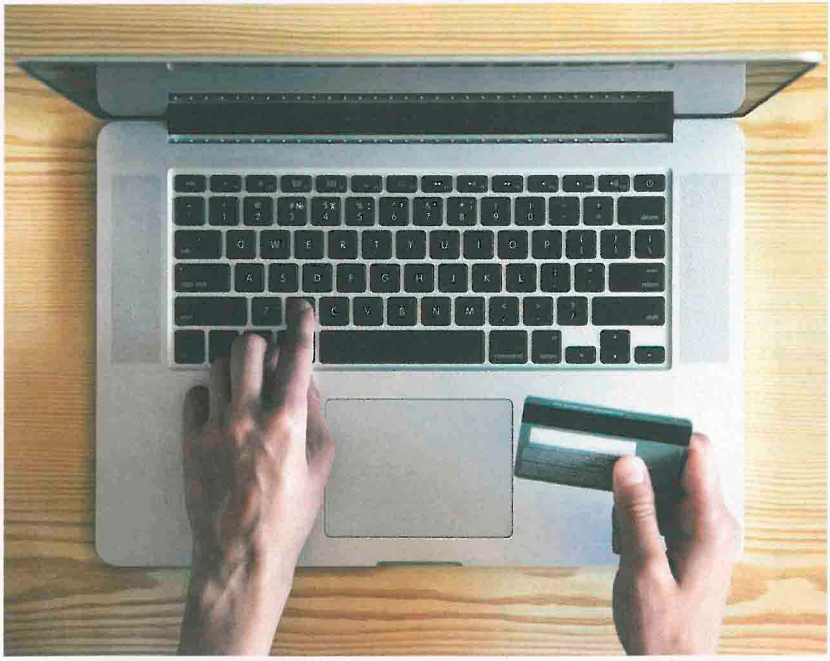
Multiple detection devices help small retailers combat fraudulent transactions

by LIZ PARKS

Large retailers like Amazon or Walmart have sophisticated payment tools running within their online shopping carts that minimize the risk of fraud and the loss of revenues and profits associated with online fraud.

But small e-commerce retailers are much more vulnerable, often lacking the broad range of fraud detection tools that higher volume e-retailers have.

John Canfield, vice president of risk for WePay, a company that provides payments and risk protection services for online platforms, notes that fraudsters have a wide variety of sophisticated processes that they deploy to commit online fraud.



That means that the best defense against them is to have a payment program that uses a wide variety of fraud detection algorithms.

TRANSACTION FREQUENCY

"Fraudsters try to hide the identity of their device," Canfield says. "When you do identity detection using an algorithm that can identify the device being used to make a transaction, you can recognize whether that device has ever been used to commit online fraud and if it has, you don't approve the sale."

Fraudsters, he explains, also often use invalid email addresses.

"That type of footprint lets a retailer know whether that email address has ever been seen before," he says. "Maybe it's been used by an honest person on Facebook or Twitter. That can be helpful in detecting fraud. A known email address indicates that the person trying to purchase something online has a reputation for honest online behavior."

Some fraudsters "are basically lazy and can't be bothered coming up with a legitimate email address so they just type in some nonsense address which, of course, doesn't guarantee that the address is bad, but if you combine that with other identification factors associated with fraud, you have another tool for detecting fraud before a transaction is completed."

Another important algorithm analyzes the frequency of transactions that are happening, one after another, within a single browser session, "to identify patterns that show someone trying to make purchases one after another in rapid succession. If one credit card is rejected, they try again with another."

WePay, which is typically not purchased by retailers but by the website platform provider building the e-commerce site, has a very wide range of fraud protection algorithms, as well as a customer user interface that is fast and easy.

That speed and ease of use, Canfield says, "results in a higher sales conversion rate and less checkout abandonment."

MEASURING ROI

Although returns on investment for WePay vary by type of business, they can be indirectly measured through enhancements in buyer conversion rates as well as significant reductions in fraud.

"If you do a good job of stopping fraud," Canfield says, "fraudsters give up and move on to someone else, so the attempts at fraud on your website go down. But if you don't have good fraud protection, fraud on your site can grow exponentially.

"Small e-retailers, not well known yet, may never have encountered fraud, but as their volume and their brand reputation grows, they can suddenly be hit hard."

Sometimes, he says, retailers suddenly hit by fraud overreact by setting up "draconian restrictions" that can create abandonment because customers don't want to experience payment processing delays.

Instead, he says, retailers "need to implement fraud protections with a scalpel, not a sledgehammer." STORES