Building defenses against the rising threat of cyberfraud

Lucy Hubbard

With each passing year, new innovations transform the business credit landscape as credit practices emerge with new technology. As credit practices evolve, risk does too, with fraudsters finding new, creative ways to target companies.

Why it matters: With the risk landscape transforming, credit managers' defenses must advance to meet the moment and protect their company from severe losses brought about by conniving fraudsters. Staying aware of cyberfraud and the many forms it takes is crucial in an industry that begs professionals to keep their heads on a swivel.

By the numbers: According to an *eNews* poll, 71% of respondents have received phishing emails from fraudsters, while 23% have seen check or credit card fraud and 6% have been the recipient of a spoofed call.

The business credit field advanced exponentially with the emergence of artificial intelligence (AI). As credit managers shift more and more of their day-to-day work to digital spaces, gaps begin to open for new forms of deception.

“We’re definitely seeing a shift in recent years. A while back businesses were mainly dealing with stolen credit cards and bounced checks, but obviously fraud has evolved,” said David Norton, risk supervisor for United TranzActions (Miramar, FL). “With the rise of digital payments, the shift has accelerated in the last few years, fraudsters have become more sophisticated, especially in how they impersonate customers or vendors while they're using cyber tactics like business email compromise and fake payment confirmations.”

Phishing emails are among the most prevalent forms of fraud; a link seemingly sent from a coworker or a request to change banking details from an email mimicking a larger customer’s business address can easily trick a credit managers accustomed to receiving an onslaught of messages.

“We receive phishing schemes on almost a daily basis,” said Brett Hanft, CBA, credit manager at American International Forest Products (Portland, OR). “Email phishing is becoming a little more challenging to identify because fraudsters are using ChatGPT, so the terminology that’s coming in from emails is a little more professional than it was originally. It used to be very easy to spot because the spelling and grammar was bad, but it's a little bit more challenging now.”

There is software available that makes it easier to report phishing emails and can send out mock phishing emails to test if members of your team notice anything suspicious. “We use it to send out test emails internally to different people at random times,” said Justin Cowart, credit supervisor at Nucor Yamato Steel Co. (Armorel, AR). “The emails look somewhat passable, so if we happen to click on a link or open an attachment on a test email, we’ve got to go through fraud prevention training.”

Phishing emails, spoofed calls and deepfake fraud may be symptomatic of new tech giving way to new fraud techniques, but new technology can also invade physical payment space. “With advancements in technology, fraudsters are now using high quality printers and stolen data from the dark web to create counterfeit checks that look realistic,” Norton said. “Some are hijacking legitimate business addresses and phone numbers to make the checks appear more authentic, which can help them bypass the verification

process. In essence, businesses are fighting fraud on two fronts, the old school paper check and the AI driven cyber threats."

Fraudsters have taken to submitting credit applications that list viable, legitimate businesses that can be verified with a credit application but include cell phone numbers and emails not affiliated with those businesses. "We are now requiring Google searches and phone conversations with the businesses from which we are receiving credit applications," Hanft said. "We are calling to say 'We've received a credit application from your company and this is the person who has submitted this application, is this person a valid employee? Did you submit this credit application and is your pending order or orders valid?'"

Taking the time to verify this information can be challenging when a salesperson is pushing for a sale to happen quickly before credit managers get a chance to verify all their information. Finding a balance between quick decision making and caution can be challenging.

"The fraudsters are really trying to push a sense of urgency. They say, 'It appears that you have this product that I can't get anywhere else,' 'I'm in the middle of a job' or 'I need this on a job site,'" Hanft said. "It's usually multiple loads of product, so it's enticing to our salesman. They're very excited about the opportunity to secure business that quickly and when the buyer stresses the urgency of needing product right now, they push credit to make fast decisions because they don't want to wait, the market is moving."

The bottom line: There is no simple approach to protecting your company from fraud, so it is important that you consider your industry, customer base and what areas of your company may be vulnerable to fraud. To be proactive in the face of fraud, regardless of what form, credit managers must be loyal to their credit policy and verification steps.