Fraud in B2B trade explained

Kendall Payton, editorial associate

B2B payment fraud is an urgent matter for credit professionals because of its scale of risk. Fraud can contribute to severe financial losses and even reputational damage for businesses. However, fraudulent activity is not always easy to catch. In fact, nearly half of all businesses take at least one month to discover the fraud that conspired.

Why it matters: Because fraud can show up in any form, it is important to catch the red flags as soon as possible. Whether through cyberattacks such as email phishing, forged digital documents, identity theft and more—credit managers must know the impacts and amount of risk involved.

One of the biggest red flags of fraud that can lead to accounts receivable losses starts as small as one typo in an email. If the email domain and company even have one letter in the wrong spot, your company is now vulnerable.

What they're saying: Tracy Mitchell, CBA, AR senior team lead at Trinity Logistics (Seaford, DE), said her company fell victim to an identity theft fraudster of one of the customers they were selling to. "The email domain of the fraudulent customer was only three letters off," Mitchell said. "People can only commit fraud where there's a gap that allows them to do that. Process gaps and insufficient security in your technology puts you at the highest risk, so if there's a lack of checks and balances, you're setting yourself up for internal fraud."

Some credit professionals will use internal controls in their credit department to help mitigate risk. For example, any changes to the company's bank information will notify a customer through a call rather than a text or sent through mail. "We have a built in a fraud check verification process in our new account's setup and no longer give out our full wire Instructions in writing," said Vimal Patel, CBF, regional credit manager at OneSource Distributors (Oceanside, CA). "We give it partially and customers or vendors have to call for the remaining portion. We run a daily credit card report that is sent out to all our sales managers and their respective operations managers so they can review and flag any potential fraud transactions before we ship out the material."

Credit card chargebacks are another common red flag that fraud is being attempted. As credit card payments become more common in B2B trade, credit professionals are more at risk for fraudsters to steal money. If a customer asks for chargebacks (a charge returned to the payer after they flag an item on their account), they can claim that the goods never arrived, or the product was not authorized by them. Fraudsters can use a digital fake card that looks like the money went through, but they are getting money back that was never sent. "There is a vast community of cyber criminals—whether individual, teamed up or government-sponsored—that are out there to get you," said Steve Winn, corporate credit manager at Marek Brothers Systems LLC (Houston, TX). "It's not a matter of if, but when you will get hit. Before, you could easily spot a phishing email by knowing the logo was fake—but now you have to dig deeper, see if the links match up or if you were expecting the email to begin with."

By the numbers:

- Cyberattacks that used stolen or compromised credentials increased 71% year-over-year in 2024, per IBM.

- 44% of credit professionals have seen an increase in fraud attempts from new customers filling out credit applications.

- Nearly 60% of B2B credit managers have experienced a customer fraudulently dispute a credit card charge.

The bottom line: Credit professionals must be more cautious and look for suspicious signs to mitigate risk and maximize profit. Setting up policies using best practices and cultivating a culture for credit professionals to feel safe and rewarded for bringing issues to light—even if it reveals their mistakes is key.

Interested in learning more? Download NACM's latest white paper, The Evolving Threat of Fraud in B2B Trade.