Texas Capital

Staying ahead of payments fraud

Our fraud experts share the latest trends they're seeing.

Despite advances in prevention, payments fraud continues to be a costly problem for businesses of all sizes. In 2023, it accounted for $102.6 billion in losses in the U.S., with check fraud alone accounting for $21 billion.[1]

The time commitment and expense involved in putting fraud protections in place can make some businesses reluctant to do so. But with fraudsters becoming increasingly sophisticated at finding weak spots in processes, IT platforms and people themselves, a comprehensive fraud prevention strategy is critical.

The good news? When organizations invest in and utilize fraud prevention tools, proven processes and employee training, fraud attempts decrease. We asked our treasury and fraud experts four questions to get their best advice and learn about what anti-fraud trends they're seeing in the market.

Meet the experts:

Nancy McDonnell
Managing Director and Head of Treasury Solutions

- More than 30 years of experience in financial services
- Driving force behind Texas Capital's commitment to innovative capital solutions and treasury management services

Robert Garrett
Managing Director and Head of Treasury Sales

- 24 years of experience in banking with a focus on treasury and client management
- Leads Treasury Sales for Texas Capital and connects teams internally to ensure a premier client experience

Stacy Nett
VP, Fraud Advisory Officer & Fraud Education Specialist

- 27 years of experience as a Certified Fraud Examiner
- 16 years working in bank investigation and law enforcement services

In what areas are fraudsters getting more sophisticated or aggressive?

Checks. "Checks continue to be the hotbed of fraud," Nett said. "Advances in technology are making it easier for fraudsters to create a more convincing counterfeit or forged item. It's so important for businesses to use Treasury Services to protect themselves, especially positive pay with payee match."

Business email compromise (BEC). "Fraudsters are looking for businesses to push the payments because banks have put so many preventative measures in place," Garrett said. "That's why you're seeing so much business email compromise and social engineering — they're looking for vulnerabilities in businesses' processes to find that one big payout."

By the numbers:

Businesses lose approximately 5% of their annual revenue to fraud each year.[2]

63% of organizations experienced some form of BEC in 2023.[3]

What do even the most sophisticated companies often miss?

The fundamentals — setting controls, creating well-defined account structure, monitoring activity daily, establishing a process for validating payment changes and not putting too much authority in one role. "A lot of people say, 'Well, I only want one bank account,'" McDonnell said. "But for businesses, you should [at least] have an account that's for money coming in and one that's for money going out."

Garrett added, "It's important to segregate duties and have a second set of eyes on payments. Typically, you want to have an initiator and a reviewer or approver. Our BankNow system reinforces this practice with user entitlements so you cannot release your own payment."

Dive deeper:

Explore other helpful fraud resources, including our fraud protection checklist.

In the digital age we live in, what is an organization's best line of defense?

Getting the right products before you need them. "A business added treasury services for checks but didn't want to invest in solutions to prevent ACH fraud. The CFO told us, 'That will never ever happen.' And two weeks later, they called me about an ACH fraud attack," said Nett, who has decades of experience in both bank investigation and law enforcement. "Now, they have everything you can think of."

Training your people. "There is a myriad of tools you can use to protect your business, but it's people who are the key to fraud prevention," McDonnell said.

By the numbers:

86% of organizations who employ end-user education and training on BEC — including how to identify spear phishing attempts — found it effective in preventing BEC fraud.[3]

Dive deeper:

See Texas Capital's full range of fraud protection tools.

How does Texas Capital help clients prevent fraud across their organization?

Taking a consultative approach. "The most valuable thing we do is act as a consultant for our clients, and that includes understanding their flow of funds and processes and marrying the two," Garrett said. "We look at [our clients'] financial infrastructure to come up with a bespoke solution that protects them with the right products for the right process."

Delivering the personal attention you deserve. "We had a case with a client who almost lost over half a million dollars," Nett said. "We were able to get the majority of the money back because of how we work to recover funds on their behalf. We have white-glove service when it comes to our commercial clients and do anything we can to recover funds."

When it comes to payments fraud prevention, a strong defense relies on your people, processes and banking relationship. Staying ahead of fraudsters can feel overwhelming, but businesses should know their banking partner will support them, whether through assessing risk, building processes with the right solutions or working to recover funds should fraud occur.

[1]Nasdaq's 2024 Global Financial Crime Report
[2]Association of Certified Fraud Examiners, Occupational Fraud 2022: A Report to the Nations
[3]AFP® Payments Fraud and Control Survey Report, 2024