Transaction security in a digital economy

How to protect your business from transactional cyberfraud

Key takeaways

- The rise in frictionless payment infrastructures and real-time transactions — enabled by increasing digital connectivity — elevates transactional fraud risk.
- A strong defense against this type of fraud requires identifying the transactional risks within your own organization and introducing friction to lower those risks.
- Establishing a clear baseline for normal payer and payee behavior can help companies detect anomalous and possibly fraudulent behavior.
- An active partnership with your financial institution can add layers of digital security and help keep key employees aware of current and emerging threats.

In our increasingly connected global economy, where financial operations have been shifting rapidly to digital platforms, the security of transactions is becoming ever more urgent. Whether it's a payment to a supplier or vendor, a receipt from a client or customer, or even an employee benefits reimbursement, every financial exchange presents opportunities for cybercriminals to exploit vulnerabilities for financial gain. And with projections that in the next decade digital technology will drive 70% of new value created in the global economy, protecting against transactional cyberfraud will remain a critical business objective.[1]

Many factors have affected the transactional fraud landscape, including more complex supply chains, the rise of cryptocurrency, the proliferation of digital platforms that enable transactions across the globe and the growing popularity of real-time payment systems that promise frictionless transactions.

What unifies these developments is the absence of a human at many points along a transaction pathway. While automation and digital connectivity have successfully accelerated payment systems, they have also reduced human oversight and opened the door for potential cyber malfeasance. Removing friction facilitates not only legitimate business operations but also new types of fraud.

Fraudsters can also exploit trust, not just in the legitimacy of the entities sending and receiving payments but also in the secure nature of the technology. The benefits of real-time payments are obvious, but can businesses reduce the concurrent risks?

[1] World Economic Forum, "Why we need to ramp up tech diplomacy to harness opportunities of the digital economy," December 28, 2023.

Strategies for managing cyberfraud risk

While it's impossible to completely eliminate transactional fraud (or any other type of financial crime), businesses of all types, regardless of their size, industry or technical sophistication, can take steps to manage the risk of cyberfraud. They can also reduce the amount of time needed to uncover evidence of transactional fraud and minimize the financial, reputational or regulatory consequences that may result from a serious breach.

There are mitigation strategies that apply to every aspect of a business's financial operations

Look for opportunities to balance convenience with friction. Many types of cybercrime depend on a lack of oversight at key points along the transaction path. Companies need to assess where the risk is greatest and determine how to introduce protections or extra steps without unnecessarily delaying transactions.

Maintain awareness of employee behavior. Historically, insider threats have been a major source of transaction fraud. Even as more transactions are automated and digitized, it remains critical that businesses maintain oversight of employees in positions to receive or authorize payments.

Stay aware of recent trends. Fraudsters focus on new transaction networks, especially where security is still catching up. Both employees who handle transactions and company leadership need to stay apprised of the current threat landscape.

Invest in security tools. While digital security tools are not a cure-all, those that monitor networks, communications and account access provide a baseline of prevention.

Understanding the risks of cyberfraud in a time of accelerated transactions

Fraud is possible in any type of transaction. While scams that trick businesses into making payments to criminal or illegitimate parties are the most common, accounts receivable (AR), merchant services and institutional transactions are all subject to risk.

The payment platforms and apps that have made transactions almost instantaneous have also introduced considerable fraud risk, and with the widespread adoption of contactless and real-time payments, the fraud can be very hard to detect. With digital connectivity between businesses and their vendors, suppliers and customers, the origins of a fraudulent transaction may exist beyond the payer and recipient.

What's more, fraudsters and criminals continue to innovate, even as they adhere to tried-and-true methods. The FBI's Internet Crime Report confirms that business email compromise (BEC)

remains a reliable scam method,[2] but criminals increasingly are setting up accounts with legitimate financial institutions, often linked to cryptocurrency accounts, to which they instruct businesses or individuals to wire payments. Given a significant increase in business-to-business (B2B) payments via the ACH network in recent years,[3] it's unsurprising that one study found that ACH credits were the payment type most targeted in BEC fraud in 2023. In fact, 47% of organizations experienced payment fraud through the ACH network[4] and numbers may be even higher since reputational risk and improbability of recovery stop many businesses from reporting losses.

It's important to remember that cash may not be the only objective of transactional fraud. Cybercriminals may use payment fraud tactics, such as BEC, to gain access to a company's data or networks for ransom purposes, to inflict reputational damage or to halt key business processes.

Here are some salient fraud risks associated with business transactions in the current environment:

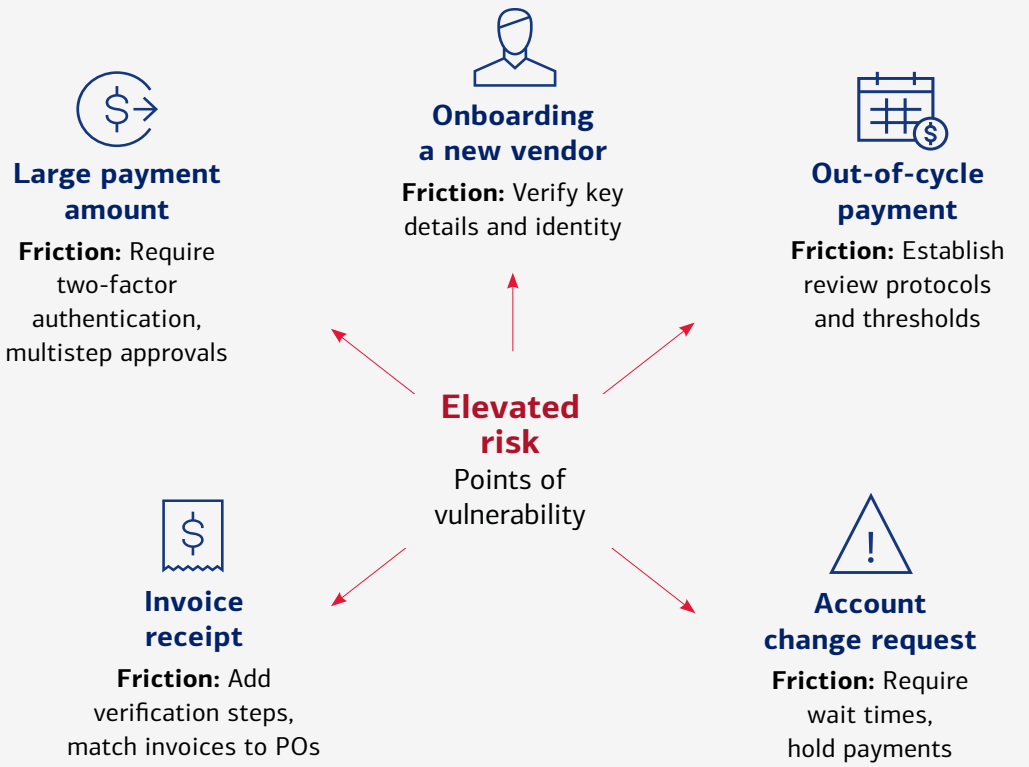
Accounts payable (AP)

Credit-push fraud — in which a business is tricked into sending an authorized payment to a fraudster — presents a growing risk for accounts payable (AP) departments. A combination of social engineering and cyber hacking can help scammers impersonate established vendors in schemes that either siphon legitimate payments from their rightful recipients or send them to entirely fictitious entities (who nonetheless hold actual accounts). Increasingly, businesses are setting up relationships with vendors that are exclusively digital, in which the friction of human-to-human interaction is completely absent, making it even harder to detect fraud.

The level of control AP departments have over payments, particularly for small businesses with limited staff or office

Reduce risk by adding friction

Slowing down at key points of vulnerability can mitigate risk across the payment transaction flow.



[2] FBI Internet Crime Complaint Center, "FBI Internet Crime Report 2023," April 2024.
[3] Nacha, "More Business to Business Payments Using ACH," July 2024.
[4] Association for Financial Professionals, "2024 AFP Payments Fraud and Control Survey Report," accessed July 2024.

locations, has thinned as they work with more international suppliers and increasingly turn to third-party financial institutions or middlemen to help execute transactions. Simply put, there are more points along a payment pathway, and each represents an opportunity for fraud.

AP decision-makers should treat every instance of unusual activity and every request from a vendor with caution. Onboarding a new vendor always carries risk, especially for companies that do not have robust policies in place for verifying the vendor's identity, such as background checks, verification of licenses, or submission of W-9s or tax ID numbers.

"Assuming the inevitability of fraud or unauthorized transactions is an essential part of any mitigation strategy."

Fraud can also take the form of account change requests and out-of-cycle or anomalous payments. In any of these situations, the fraudulent request may come from an out-of-band email that appears legitimate, or the fraudster may have gained access to the vendor's email account.

Accounts receivable (AR)

Traditionally, accounts receivable (AR) departments have focused mostly on protecting against internal fraud such as pocketing payments that are written off as losses, manipulating balance sheets, "kiting" (transferring funds from one account to another to cover a theft) or absconding with overpayments. While these schemes are still business risks, digital connectivity has led to other types of scams — perpetrated by external parties — becoming more prevalent.

For example, payments made with stolen credit card numbers may not always have a financial impact on a business, but criminals can take the process a step further by engaging in an overpayment scam, in which a fraudster makes a payment for goods or services that exceeds the asking price and requests that the overpayment be refunded to them in cash. Because the initial payment is fraudulent, any refund represents an actual gain for the fraudster, who can then get away with the cash. With the increase in real-time payment rails and international payment integration systems, criminals can execute fraud and money laundering schemes before AR staff are able to spot any irregularity.

Fraudsters' ability to create convincing identities can extend to shell companies that offer to recover delinquent payments. Instead of collecting outstanding debts for a fee, the scammers simply collect and disappear, leaving the original company little recourse for recovering the funds.

Employee benefit accounts

Retirement accounts and other employee benefits represent a ripe opportunity for criminal actors. Often containing substantial funds and extensive personally identifiable information (PII), these accounts are typically maintained digitally and are accessible by the employer and the employee. Both sides can experience threats.

By downloading malware or through social engineering, criminals can either bypass company security or trick administrators into believing that actual employees, or former employees, are making legitimate requests to confirm sensitive information, make withdrawals, or close an account and transfer the proceeds. In some cases, a fraudster takes out a loan against the account. Others may trick an account holder into revealing account information under the guise of plan maintenance or a bogus security alert.

Employees risk significant financial losses or compromise of their PII. But companies maintaining the plans can also face severe consequences in the form of fines for lack of fiduciary compliance. Breaches to health information could result in violations of the Health Insurance Portability and Accountability Act (HIPAA).

How to mitigate transactional fraud risk

A proactive defense against transactional cyberfraud requires acceptance of a basic premise: Any company of any size could at any time discover evidence of a fraud or unauthorized transaction that has already been committed or is in progress.

Cyber fraudsters can be just as stealthy as perpetrators who relied (and still rely) on conventional methods such as check forging, kiting and account skimming — and the speed of digital transactions often works to their advantage. Assuming the inevitability of fraud

or unauthorized transactions is an essential part of any mitigation strategy. A slow, ineffective response to a cybercrime often can reflect a lack of planning and comprehensive risk management.

The assumption that fraud will happen can be thought of as a business adaptation of the zero-trust architecture[5] that cyber security professionals apply to enterprise protection, and it can apply in ways that are specific to AP, AR and benefits transactions, as well as across digital payment systems.

Accounts payable

Effective defense against AP fraud begins with recognizing that cyberfraudsters have observed the shift to ACH payments and ramped up activity in response. Employees receiving an invoice or request for payment from an established vendor — even one that matches their known contact information — can no longer assume the communication is legitimate.

When onboarding new vendors, employees should take the necessary time to record and verify key details, such as company or personal information and the routing numbers and contact information of the financial institution to which the vendor directs payments. If the account is held with an overseas bank, employees can search for an International Bank Account Number (IBAN) or consult the Federal Reserve for information.

AP departments can also create friction by establishing review protocols and thresholds for any requests to change accounts or process out-of-cycle payments. Rather than framing the process as a delay, AP staff can present it as a necessary step to ensure the security of the vendor's accounts as well as their own.

Reduce risk by pausing for anomalies

Protect accounts receivable transactions by paying close attention when you see:

- Requests for refunds or payment voids
- Notices of overpayments
- Unusual communications
- Digital transactions of unusual size, cadence or origin

Accounts receivable

AR departments can institute cyberfraud detections by focusing on anomalies. Those could include requests for refunds or payment voids, notices of overpayment, communications from vendors who claim to have paid their balances yet are still receiving payment requests, or a resumption of payments from long-dormant accounts. Any single anomaly may be evidence of cyberfraud, and a trend of unusual requests or activity could indicate an ongoing scheme.

As with AP, AR can benefit by reviewing the activity of established payees as frequently as possible. They can also perform regular audits to flag digital transactions (payments or refunds) of unusual size, cadence or origin.

Employee benefit accounts

Companies that rely on a third-party administrator (TPA) to manage employee benefit plans, most notably retirement and health savings accounts, need to manage the risk this extra layer of digital connectivity creates. Referring to or conforming with a higher compliance standard, such as the System and Organization Controls 2 (SOC2) framework of the American Institute of CPAs[6], can help businesses assess their digital and data-sharing protocols with TPAs and determine where they might need stronger defenses.

Since the account holders themselves present one of the greatest risks to the security of their data and funds, businesses should consistently advise employees to use two-factor authentication and biometrics, refresh passwords regularly and protect their PII. Administrators must operate with the same level of caution regarding digital communications by confirming the legitimacy of any request for account information. Unless a request is made in person or the account holder's identity can be verified through alternate channels, it's safer to assume the request is fraudulent.

Working with financial institutions and platforms

Efforts to protect against cyber transactional fraud also depend on financial institutions and organizations such as Nacha, which governs the ACH network. But the responsibility for security

is not a one-way proposition. For instance, Nacha encourages information sharing among all parties affected by wire transfer

[5] NIST, "Zero Trust Architecture," August 2020.

[6] American Institute of CPAs, "SOC2® - SOC for Service Organizations: Trust Services Criteria."

fraud, arguing that it helps educate end users while also assisting participating institutions in protecting a critical digital network.[7]

As more companies deal with complex supply chains and global payment arrangements, working closely with the financial institutions that hold their accounts and enable transfers is another important factor in security. Every organization should explore the services their financial partners can offer to protect digital transactions and help with forensics and recovery after a payment fraud or data breach occurs. ■

[7] Nacha, "A New Risk Management Framework for the Era of Credit-Push Fraud," September 2022.