4 Steps to Mitigating the Risk of Payment Fraud

paymerang℠

4 Steps to Mitigating the Risk of Payment Fraud

Payment fraud is insidious.

- It chips away at corporate profitability.
- It jeopardizes your corporate reputation.
- It consumes staff time with remediation.
- It erodes the trust of your trading partners.
- It puts your business' viability at risk.

Not surprisingly, mitigating the risk of payment fraud and data breaches is a major undertaking – and an increasingly big headache – for the accounting team responsible a business' financial well-being.

A single fraudulent incident can consume weeks of an accounting team's time as they determine the financial impact, attempt to recover the funds, plug security gaps, and work to repair reputational damage.

With internal and external threats on the rise (think: Business E-mail Compromise or BEC attacks), accounting teams have no time to lose in developing a holistic approach to mitigating the risks of payment fraud, safeguarding sensitive banking information, and ensuring the integrity of the accounting system.

This white paper provides a four-step plan to help accounting teams accomplish that.

The Growing Threat of Payment Fraud

A record 82 percent of organizations reported payment fraud incidents in 2018. That's according to the 2019 Association of Financial Professionals (AFP) Payments Fraud & Control Survey.

Large enterprises are particularly vulnerable to payment fraud attempts. An eye-popping 87 percent of businesses with greater than $1 billion in revenue were the target of payment fraud in 2018, AFP finds. Sixty-nine percent of businesses with less than $1 billion experienced payment fraud attempts.

BEC attacks – schemes that use bogus e-mails to trick businesses into initiating payment – account for a growing share of payment-fraud attempts. Eighty percent of companies reported BEC fraud attempts last year with 54 percent of businesses suffering financial losses as a result of BEC, AFP's research finds. A single BEC scam can result in losses of more than $1 million for a medium-sized business.

While the percentage of businesses exposed to check fraud declined slightly in 2018 (43 percent of businesses), AFP finds that checks continue to be the payment method most impacted by fraud.

A Four-Step Strategy for Mitigating Risk

Soaring payment fraud should be a wake-up call for accounting teams.

There are four steps that businesses can take to help mitigate the risks of payment fraud:

Step 1: Protect the Payment

Step 2: Secure the Operations

Step 3: Fortify the Network

Step 4: Lock Down Compliance

Addressing each of these steps will help businesses secure their payments and sensitive information.

protecting the payment

The first step to mitigating the risk of payment fraud is to Protect the Payment.

Electronic payment solutions, such as virtual cards and ACH transactions, provide greater protections than paper checks, mitigating the risk of payment fraud. Electronic solutions allow for defined roles and permissions and privileges, separation of duties, configurable business rules, complete audit trails, hierarchical access, administrative controls for security settings, and parameters (such as the amount, supplier, location, or date) for approved payments. Some advanced electronic payment solutions also automatically alert users to suspicious payments.

Virtual Cards ("vCards") are designed with security in mind. Every vCard payment is designated for a single use and is only valid for a certain supplier, date range, amount or other criteria that helps prevent misuse; businesses don't have to worry about lots of high credit-line cards being in circulation. A vCard can never be charged for more than it was authorized for. And unlike ACH transactions, vCard payments don't require suppliers to provide their banking account information to customers. Finally, suppliers know when a payment will arrive, buyers know the status of each vCard payment to suppliers, and the payee on a vCard payment cannot be changed.

These are the reasons that vCards are the most secure form of payment that businesses can make.

ACH is another method for making secure payments. The controls built into ACH payment solutions (such as dual approvals and segregation of duties) help mitigate the possibility of fraud. With ACH payments there also is little chance of the payment being intercepted or "washed." And trusted third parties with a highly secure infrastructure can safeguard supplier banking data. Internal process improvements will help to further protect ACH payments. Businesses should take precautions to verify suppliers against information in shared data sources before enrolling them in the ACH payment network. Data protection can be further enhanced through two-factor authentication of vendors that log into payment portals, and by encrypting banking information (restricting access to viewing or changing that information across the enterprise).

Even paper checks – which represent the lion's share of financial losses from payments fraud, per AFP's research – can be better protected when combined with a positive pay service from a financial institution. A positive pay service verifies the accuracy of a check's dollar amount, date, and check number when it is presented for payment, thereby protecting against counterfeit and altered checks.

Regardless of the payment mechanism used to pay suppliers, buyers should take care to validate the identity of suppliers who are requesting changes to their banking information, to ensure that the person is not an impostor attempting to commit fraud. Strictly limiting access to card and banking information also helps prevent the possibility of data theft or nefarious activities by insiders who are working with fraudsters.

securing the operations

The second step to mitigating the risk of payment fraud is to Secure the Operations.

Accounting teams must safeguard sensitive banking information by keeping it out of the open; implementing a clean-desk policy with consequences for policy violators. Check stock should always be kept under lock and key. And a certified shredding service should be used to appropriately destroy documents with sensitive data when they are no longer needed and to bring discipline to document retention.

Additionally, employees who are involved in supplier payments should be made aware of the internal and external threats (including cyber and social engineering schemes) to sensitive information. Quickly detecting suspicious activities and transactions is critical to stopping crooks in their tracks and/or recovering funds.

Also consider implementing an electronic payment solution that assesses the potential risk of payments based on a variety of criteria (amount, frequency of payment, supplier history, etc.) and assigns a fraud score. For instance, any payment that is sent to a new bank account or address should be more closely scrutinized.

Accounting teams should also establish operational procedures and controls for the execution of payments, including multiple approvals, payment limits, segregation of duties, and rotation of job responsibilities.

Finally, accounting teams should ensure that all employees responsible for paying suppliers are properly trained, with regular refreshers. The people who execute supplier payments are an important line of defense for combatting fraud. Staff should be regularly trained on known fraud schemes and on how detect suspicious links or e-mail addresses. Ongoing information on payment threats will help staff respond more quickly to new schemes. And impress upon staff to always verify information when in doubt!

fortifying the network

The third step to mitigating the risk of payment fraud is to Fortify the Network.

Rising cyber threats drive home the importance of safeguarding your network.

Start by ensuring that the PC used to generate payments is kept in a protected "clean room" environment. This helps ensure the integrity of the environment used to process payments. Next, implement advanced anti-virus applications to detect and quarantine any malware that may have reached the PC used to generate payments. And strictly limit the application software that you allow to run this PC. The goal is to limit the possible installation of malware that steals business banking information or bank account login data.

Securing e-mail communications is another way to fortify the network. Buyers and sellers increasingly communicate via e-mail. But trading partners must be confident that the e-mails they receive can be trusted, and do not include any malicious applications. This is especially true in the case of sophisticated BEC scams that use the identity of actual suppliers to trick buyers into making payments to fraudsters. Accounting teams should use secure e-mail communications, where e-mail is held and then retrieved by the recipient, instead of being transmitted in an unsafe manner across the Internet (from mail server to mail server).

A vulnerability management program is another way to fortify the network. These programs identify security weaknesses across the enterprise technology landscape and suggest remediation/actions to strengthen the security profile of these technologies. A vulnerability management programs reduces the chances that bad actors will exploit these weaknesses and compromise a technology environment, to steal sensitive and proprietary data. A vulnerability management program can start with conducting security scans and reviewing security configurations to identify outdated, vulnerable software and weak configurations. Once risks to your technology environment have been identified, remediation actions may take the form of software patches or upgrades, the implementation of new software, or the reconfiguration of technology.

Small businesses that cannot afford a full-blown vulnerability management program should ensure that they always use the most up-to-date version of their payment and accounting applications.

Finally, businesses should implement technology to detect threats across their network. Detecting and acting on possible intrusions to your network environment helps protects network integrity and confidentiality. Networks today should be designed so that if there is a compromise, it is prevented from spreading. When combined with network activity logging, threat detection is a big step toward thwarting cybercrime.

locking down compliance

The fourth step to mitigating the risk of payment fraud is to Lock Down Compliance.

Businesses require compliance oversight and audit assurance, no matter the payment mechanism.

NACHA is the trustee of the ACH Network. NACHA helps with careful development, administration and rules required to operate the network. Financial institutions and enterprises use the NACHA Operating Rules as a guide to keep the network effective. For participants in the ACH Network, NACHA requires an annual Operating Rules compliance audit as an oversight activity.

A Service Organization Control (SOC) assessment is another form of compliance safeguard that can be used as an audit assurance function. During a SOC assessment, an audit expert is hired to review and attest that an organization's governance and control structure appropriately handles requirements for:

- Trust Services Criteria of Security
- Availability
- Processing Integrity
- Confidentiality
- Privacy

A clean SOC-2 report means companies can depend on their provider for secure, compliant service operation.

PCI compliance is another way to lock down compliance.

The Payment Card Industry (PCI) Security Standard Council, which includes Visa, Mastercard, JCB, Discover, and American Express, requires organizations that collect, process, or store credit card information to implement a set of security control standards to protect this information from falling into the wrong hands. The PCI Data Security Standard, also known as PCI-DSS, details 12 security control areas that must be implemented into the payment card data environment. The PCI compliance rigor is based on the number of credit card transactions

performed, with the highest transaction levels requiring an annual certification compliance audit into the 12 PCI-DSS control areas by an audit expert, quarterly security scans, an annual penetration test, and completion of a self-assessment questionnaire with attestation.

Finally, the US Treasury Watchlist is another tool for locking down compliance. The Office of Foreign Assets Control (OFAC) manages lists of individuals and organizations that have been identified as threats to U.S. National Interests; payments cannot be made to any party on this sanction list. If a positive match is identified, then the payment is to be blocked and the OFAC is to be notified within 10 business days. Accounting teams should ensure that they have a way to check suppliers against the OFAC list.

The Bottom Line

Businesses have too much at stake to leave themselves vulnerable to soaring payment fraud. A single fraudulent incident could cost a business big money. And accounting teams could lose weeks of valuable time investigating and remediating payment fraud. Developing a holistic risk management strategy provides accounting teams and the businesses they work for with the upper hand against bad actors.

About the Sponsor

This white paper was sponsored by Paymerang.

Paymerang is a leader in accounts payable automation. Their award-winning electronic payables solution provides a simple and secure way for enterprises to pay their vendors.

Through its revolutionary simplicity, Paymerang enables companies to pay their vendors electronically with a single payment file. By handling the entire process, from secure vendor enrollment to payment delivery to reconciliation and customer service, Paymerang is able to offer efficiency that saves thousands of hours of finance time, security that protects all types of payments from fraud, and financial rewards that turn accounts payable into a profit center. The company provides solutions for enterprises around the country in education, healthcare, finance, media, manufacturing, services, and beyond. By implementing Paymerang, accounting departments gain transparency and can refocus efforts on more strategic priorities like operational efficiency and financial controls.

| business payments **made easy.**