Simple Ways To Mitigate Fraud Risk In Accounts Payable

A MineralTree Topic Paper

mineraltree®
AP and Payment Automation

Businesses now face increasing fraud risk, creating significant challenges for accounts payable teams. In 2017, 78 percent of businesses were negatively impacted by payments fraud and suffered from financial losses, reductions in efficiency and damage to the corporate brand image.

Traditionally, AP risks were addressed with manual, email-based approval processes designed to verify all invoices and payments. However, these processes are very challenging to scale as the number of invoices and payments being made goes up. As a result, businesses are left exposed to fraud more and more often as accounts payable teams become more and more swamped.

Businesses must recognize the risks involved in their AP department, understand the typical types of fraud that occur, and take realistic steps to protect themselves from increasingly tech-savvy criminals. This whitepaper will address the major risks that businesses face, as well as a series of simple approaches that businesses can incorporate to effectively mitigate those risks.

Major Risks, Major Costs

While the risks to the AP process may display some variation in scope and size, they are all constructed around three basic types of criminal activity.

Check Fraud

Statistics show that check fraud is on the rise, with an estimated $1 billion in victim losses (there were actually about $7 billion in attempted fraudulent checks, but banks have stopped payment on about $6 billion).[1,2] A survey from the Association for Financial Professionals indicated that 74 percent of businesses have suffered from some variety of check fraud.[3] This type of criminal activity can be propagated by an internal or external source to the business and can occur in a variety of ways.[4,5] Examples of ways that check fraud can occur include forgery, counterfeiting and alteration, which are becoming increasingly difficult to detect with improvements in software programs and printers.

[1]https://www.aba.com/Products/Surveys/Pages/2017-Deposit-Account-Fraud.aspx
[2]http://frankonfraud.com/fraud-reporting/top-10-fraud-losses-for-2016-and-where-they-are-headed-now/
[3]http://dynamic.afponline.org/paymentsfraud/p/1
[4]http://www.auditnet.org/audit-news/articles/accounts-payable-fraud-10-ways-to-identify-it
[5]http://www.ckfraud.org/ckfraud.html

Business Email Compromise (BEC)

In 2017, the FBI estimated that BEC fraud resulted in victim losses of over $676 million, making it one of the most common types of fraud.[6] BEC, which is based on social engineering principles, is a rather sophisticated, targeted scam, since it involves a keen understanding of how a business operates. Fraudsters choose a business and then investigate the chief executive officer or decision makers as well as lower-level employees in the AP department. The fraudsters then identify a time when the decision maker is out of the office, either on vacation or business, and then reach out to the targeted AP employee. The demand for an immediate transfer of funds can come via phone call, but it is more common for it to come through an email with a fraudulent address that looks very similar to the decision maker's address. Employees will assume that the transfer of funds is urgent since the request is being made while the decision-maker is out of the office and will quickly perform the action.

Automated Clearing House (ACH) Fraud

ACH fraud can be extremely difficult to defend against. This type of fraud includes elements of social engineering as well as an understanding of a company's basic verification practices. In ACH fraud, criminals contact a business or organization and make a request to update a vendor's payment information. Sometimes these requests include a change to an account and routing number or to change the payment method from check to a wire transfer (which includes the new account and routing numbers). When valid payments are made, the money goes to the updated account, creating a loss for both the actual vendor and paying business. Fraudsters then quickly move the funds to another international account or remove them from the specified account.[7] While some companies do include verification procedures for validating updated payment information, these are typically not adequate to address this criminal activity since they do not always include an automated response system.

[6]https://www.fbi.gov/news/stories/2017-internet-crime-report-released-050718
[7]https://www.nacha.org/news/ach-operations-bulletin-1-2017-social-engineering-fraud-against-public-sector-and-other

Traditional Approaches To Fraud Protection In AP

Businesses have traditionally employed homemade approaches to fend off AP fraud with varying degrees of success. The standard approach involves email threads that track approvals for the payment of invoices. These methods may work to some degree, but are not repeatable and scalable. As a business continues to grow and add more vendors, they are left exposed as the accounts payable team struggles to track all of the outstanding invoices carefully, and can mistakenly pay a duplicate invoice, or an invoice that is entirely fraudulent altogether.

Another attempt to manage risk involves the utilization of approval rules. In this mitigation scenario, specific payment amount regulations are hard coded into the accounting system. While this approach can somewhat help reduce the incidence of fraud, it is not foolproof. Fraudsters merely need to create invoices for less than the specified approval amount to move fraudulent invoices through the system. Fraud can also occur through understanding the approval process. For example, if approval is needed for any amount over $10,000, invoices may appear that are just under the approval amount.

Many companies that refuse to move beyond traditional risk mitigation practices cite the lack of funds to invest in an automated AP system, a small volume of invoices, and a lack of information technology and leadership support. However, a more proactive approach to fraud detection can pay off tremendously, as the early detection of fraud reduces the financial consequences to a company. There are a variety of simple, effective approaches to mitigating risk in AP.

Effective Solutions To Mitigate Risk

Segregation Of Duties

Segregation of duties involves breaking up the payment process into multiple steps, with a different employee responsible for each separate step. The segregation of duties distributes critical aspects of the invoicing and payment process through a shared responsibility model.

This practice ensures that no single employee has total control over money moving in and out of a business's bank account, and checks their power against other employees within the company.

Dual-Factor Authentication

In this scenario (also referred to as two-factor authentication), the process involves the utilization of two important pieces of information to verify the identity of the employee responsible for releasing funds. Commonly, this involves the utilization of a password and another security code delivered via email or text message.

This practice adds another layer of security, by requiring employees who approve payments to enter a unique security code that they receive via text or email every time they release funds

Tokenization

Tokenization is a payment control that produces a unique credit card number for every vendor payment that you make. That credit card number can only be used once, and only for the amount that you designated for that specific payment. In a world that is full of variability, tokenization enables you to drastically mitigate the risk of your company credit card information falling into the wrong hands.

Purchase Order Matching

Purchase order matching is an effective approach to mitigating risk. In this approach, invoices can be matched with purchase orders in three different ways. The first is the simplest: two-way matching. This simply matches the correct invoice with its purchase order. Three-way matching occurs when the invoice, purchase order and receiving information are matched. Finally, four-way matching occurs when the inspection information, receiving information, purchase order and invoice are all matched.

This practice guarantees that the invoice that gets paid matches the initially agreed upon amount, and enables businesses to bypass the process of verifying invoices with department heads.

Positive Pay

Positive pay is a cash management service offered by banks. A company that is issuing checks sends a list of those checks to the bank for verification, and this list includes important information, such as the number of the check, amount it was made out for and date it was issued. When the checks are presented to the bank, the bank examines its register list to ensure compliance.

Checks that do not match what the bank has on file will automatically generate a hold on the funds until the company can verify or negate the presented check. Although this is an effective way to catch fraud, it does involve some additional cost.

Company Culture

Finally, effectively managing behaviors at your business involves an examination of your company culture.[8] While this approach to mitigating risk will involve a long-term commitment to creating a transparent work environment, it will pay off in the form of less negligent behavior, such as skipping parts of an SOP or failing to comply with established regulations.

[8]http://smallbusiness.chron.com/effects-negative-corporate-culture-ethical-behavior-65787.html

Automation Significantly Reduces Fraud

Automating the AP process offers businesses the opportunity to build all of these best practices into their accounts payable process in a scalable and repeatable manner. Businesses can choose from a variety of sources to mitigate risk, but a single-source solution, such as MineralTree, has been shown to be very successful at helping to limit risk and improve efficiency.

For example, AP automation builds segregation of duties into the accounts payable workflow. Solutions like MineralTree utilize online workflows with distinct manager and approver rules to create segregation of duties, and the manager and approver rules can be modified according to need or type of invoice, allowing for the maximum flexibility and security within the AP system.

AP Automation solutions like MineralTree also incorporate dual-factor authentication into everyday accounts payable. Since two unique pieces of information are required (typically, a password and another identifier, such as a numerical code or token), this measure helps to prevent unauthorized access when a password is compromised.

While manually checking purchase orders and invoices is a tedious process, AP Automation solutions provide automated purchase order matching to streamline matching and eliminate opportunities for errors.

Additionally, by providing easier access to electronic payments, AP Automation solutions also eliminate the need to pay with paper checks. In some cases, solutions also have built in virtual card payment options that include tokenization, ensuring that the strongest protections are applied to credit card transactions. Solutions like MineralTree also allow for the secure review and release of payments on-the-go, which provides fast-moving businesses with the flexibility and security that they need regardless of location.

Take The Next Step

Are you curious to see what your team looks like with these payment controls in place? Set up a demo with MineralTree and get a free assessment of your current risk of fraud. Contact us today at 617.299.3399 or email info@mineraltree.com.

SWMF- (10302018)