SPRING 2017, ISSUE 3

INSIDE THIS ISSUE

VENDOR FRAUD
PAGE 1

Practice Tips
PAGE 6

FVS EYE ON FRAUD

The AICPA Forensic and Valuation Services Quarterly Report on Fraud Trends and Topics

VENDOR FRAUD

Issued by AICPA FLS Fraud Task Force
Lead Author: Amy Yurish, CPA

Vendor fraud continues to be a significant threat to organizations. "Vendor, supplier, and procurement fraud" was cited as the second most prevalent fraud in the past 12 months by the 2016–2017 Kroll Global Fraud Annual Report.[1] Further, technology has added a new layer of complexity in fighting vendor fraud. Many times, the most damaging vendor fraud schemes involve a cyber component that exploits an organization's vulnerabilities in its IT systems, making these schemes more complex than ever to defend against.

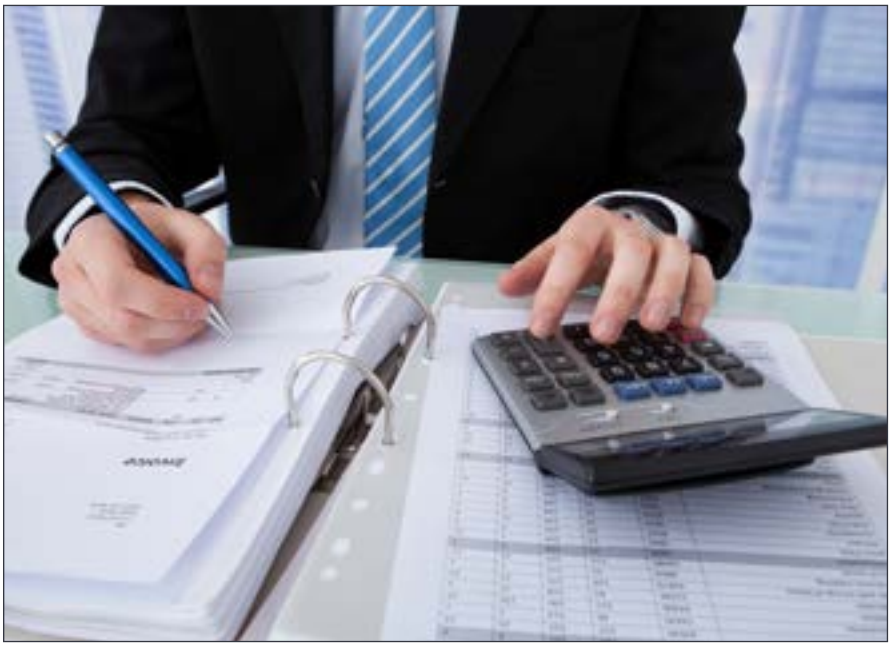
Business email compromise, in which fraudulent emails are sent in the names of business executives or vendors to solicit unauthorized wire transfers, was identified by the Internet Crime Complaint Center in its 2015 annual report as the number one cyber fraud in terms of losses, resulting in losses of more than $246.2 million for companies in the United States.[2] Additionally, according to a survey conducted by PricewaterhouseCoopers, the PwC Global Economic Crime Survey, although procurement fraud is generally down from 27 percent to 22 percent, the United States experiences a disproportional amount of cybercrime (including vendor-fraud-related cybercrime) compared with the global market (54 percent in the United States compared to 32 percent globally.)[3]

At the same time, perpetrators have become more sophisticated in adapting to the challenges associated with more robust internal control environments designed to prevent, detect, and deter fraud. Greater awareness, coupled with increased scrutiny by auditors due to the requirements of the Sarbanes-Oxley Act of 2002, have made it more difficult for individuals to perpetuate basic vendor fraud schemes that were prevalent in the past against large, SEC-registered entities. However, this has not seemed to deter the more sophisticated fraudsters, who see breaking through enhanced internal controls as a challenge, not a deterrent.

Fraudsters have access to the same publications and guidelines that have helped organizations become more familiar with necessary internal controls. Thus, many times, perpetrators are as familiar as organizations are with the very types of internal controls intended to prevent them. The rise of cloud computing and digital data has presented these individuals with new opportunities to take advantage of weaknesses in an organization's internal controls and IT

Continued on page 2

[1] *Kroll Global Fraud & Risk Report: Building Resilience in a Volatile World 2016/2017.*
[2] *Federal Bureau of Investigation – Internet Crime Complaint Center, 2015 Internet Crime Report.*
[3] *PwC Global Economic Crime Survey 2016: U.S. Results.*



Vendor fraud schemes vary greatly in their sophistication and complexity. The amount of damage caused to an organization is typically commensurate with the inherent sophistication of the scheme. More sophisticated vendor fraud schemes are harder to detect and sometimes take years to unravel, at which time, the fraud has likely already cost the entity substantially.

systems. The challenges to deterring vendor fraud have never been greater, and the education on vendor fraud is ever-evolving, along with the constant changes in technology.

What Is Vendor Fraud?

Generally, vendor fraud includes abuses that involve improper payments to real or fictitious vendors. In vendor fraud, perpetrators manipulate a company's accounts payable and payment systems for personal gain. They do this in many ways, and these methods can be categorized into three major groups:

- Fraud committed by an internal employee, or multiple employees, through collusion, against the defrauded organization
- Fraud committed by an outside vendor or individual working without insider support
- Fraud that involves collusion between an outside vendor or individual and an internal employee or multiple employees

Some examples of red flags that could indicate vendor fraud are as follows:

- Multiple invoices paid to one vendor on the same date or within the same payment cycle or multiple invoices for the same amount paid to the same vendor
- Sequential invoice numbers from the same vendor and payments authorized during unusual times (dates or hours outside of normal operating business hours)
- Differences between contract terms and invoices received from a specific vendor, for example, if the total payments made to a specific vendor exceeds the contractual limit

Who Is at Risk?

Small- to mid-sized private entities — so-called "soft targets" — generally face greater risk of exposure for vendor fraud schemes. These businesses are less likely to have robust internal controls or internal audit functions in place. Further, these types of organizations typically rely heavily on a few employees to execute the vendor and payment functions and lack prudent segregation of duties. This increases the opportunity for one or two individuals to manipulate payments and records without easily being caught.

Due to the requirements imposed by Sarbanes-Oxley on SEC-registered entities, larger organizations typically have risk assessments and strong internal controls in place. This makes these organizations harder targets for individuals seeking to circumvent the processes and procedures for personal gain. However, although larger organizations typically have

Continued on page 3

periodic financial statement audits conducted by external auditors, these cannot be relied upon to detect fraud or offer assurance that fraud does not exist. Financial statement audits are designed to provide an opinion on specified criteria, which typically includes whether financial statements are stated in accordance with specified accounting standards and whether they are free from material misstatements. It is the organization's management that is responsible for implementing processes, procedures, and internal controls to mitigate and detect fraud.

Examples of Vendor Fraud Schemes

Vendor fraud schemes vary greatly in their sophistication and complexity. The amount of damage caused to an organization is typically commensurate with the inherent sophistication of the scheme. More sophisticated vendor fraud schemes are harder to detect and sometimes take years to unravel, at which time, the fraud has likely already cost the entity substantially. The following provides examples of vendor fraud schemes, varying in sophistication from basic to complex, involving a cyber element.

Employee Skimming

This type of fraud scheme involves individual employees using an unsophisticated and low-level approach to vendor fraud. Typically, an employee will use unauthorized methods to skim small increments of money. Examples of this type of scheme include overstating the quantity of goods invoiced from an organization and skimming the excess goods or overstating the total cost of an invoice and skimming the excess cash. In this type of scheme, an employee may overstate an invoice. For example, an employee enters an invoice with inflated amounts and then pays the original amount to the vendor plus the inflated additional amount to himself. The opportunity for this type of scheme is increased when the same employee has access to both the invoice creation and payment systems. The potential for this type of fraud scheme will always be prevalent within an organization due to the simplicity of the scheme and ease of access for employees. Fortunately, because of their unsophisticated nature, these types of schemes are typically easier to detect and usually involve low dollar amounts.

Fictitious Vendor Schemes

In this type of fraud scheme, an employee creates false vendors and invoices in order to direct payments to themselves or a related party. These are commonly referred to as fictitious vendors, shell companies, or phantom vendor schemes because the employee directs payments to a vendor that does not exist. Signs of a fictitious or phantom vendor scheme are payments made without supporting invoices, payments made to photocopied invoices rather than originals, or suspicious vendor addresses, including P.O. boxes.

Vendor Schemes Involving Legitimate Vendor Accounts

These schemes involve actual vendors that an organization uses and are perpetrated in a number of ways. Many of these schemes require employee collusion in order to effectively execute the fraud scheme. A few examples of vendor schemes involving actual vendors are as follows:

- Duplicate invoicing for goods or services when a vendor is charging an organization for the same goods or services twice
- Overbilling for legitimate goods or services when a vendor invoices an organization for higher quality goods than what was delivered or a more complex service than what was performed
- Bribes and kick-back schemes involving collusion between a vendor and an employee within an organization when the two individuals work in

Continued on page 4

conjunction to perpetrate the fraud (the employee is incentivized by receiving a bribe or kickback from the vendor)

- Bid rigging between two or more vendors, including bid suppression, complementary bidding, bid rotation, and so on, allowing vendors to work together to fraudulently manipulate the procurement process
- Price fixing between two or more outside vendor companies to establish a price range or minimum price for goods or services in order to attempt to increase the market price of the specific goods or services

Outside Cyber Intrusion

The most complex—and hardest to detect—vendor fraud typically is perpetrated by an outside entity unknown to the victim organization or its employees. It involves the use of a real, legitimate vendor account, but one unknown to that vendor. In these schemes, the perpetrator accesses an organization's vendor and payment records electronically to manipulate the data to skim payments based on legitimate invoices and purchase orders. For example, ABC Company purchases goods on a regular basis from D Manufacturer and pays D Manufacturer based on its monthly invoices. A third-party electronically changes the invoices slightly to increase the amounts due and then directs the additional amount due to a separate bank account under their control. ABC Company continues to pay without noticing the slight increase in cost, and D Manufacturer continues to receive the amount expected from its own records while the perpetrator is receiving the differential. Typically, changes are also made to the return and sales allowances accounts to make it more complicated to verify invoice amounts and records. These types of fraud schemes are hard to detect, even when organizations have strong internal control frameworks and internal audit functions.

Case Studies

The following are examples of real cases of vendor fraud. These cases demonstrate different scenarios and schemes of vendor fraud at varying levels of complexity and sophistication.

Fictional Vendor Embezzlement Scheme

John H. Martinez, a telecommunications administrator, pleaded guilty to defrauding his employer, Lincoln Land Community College, of approximately $700,000 over seven years by authorizing the order of various products with a forged supervisor's signature. Not only was Martinez forging his supervisors' signatures to authorize expenditures over a certain amount, he would intentionally mail checks to fictitious vendors or fictitious addresses, or both, knowing the checks would be returned to him due to invalid addresses. Once returned, Martinez deposited the checks into his personal bank account. Additionally, some of the vendors were owned by Martinez's friends, who would deposit the checks into their own bank accounts and split the proceeds with Martinez.

$2.3 Million Embezzlement Scheme

Kimberly Jean Miller pled guilty to tax evasion for failing to report income she unlawfully received from her employer. Miller was the director of finance at the University of Miami's Rosenstiel School of Marine and Atmospheric Science (RSMAS) from 2002–2012. Over the course of her employment, Miller embezzled $2.3 million by falsifying invoices from a legitimate vendor called International Assets. Miller changed the International Assets invoices so that the vendor name would appear as "Inter, Inc." on the payments. The checks would be mailed back to RSMAS, and then she would deposit the checks into a separate business account in the name of Intercontinental Oceans, Inc., which she controlled. Miller was sentenced to three years in prison in August 2016.

False Invoice Skimming

Robert Banks, a carpenter and locksmith for the Plainfield Board of Education, admitted to defrauding his employer, stealing nearly $20,000. In his role, Banks was responsible for purchasing carpentry supplies from vendors. The board entered into contracts with a vendor, Bayway Lumber, to purchase certain products at a discounted price. From 2007–2015, Banks worked with the employees of Bayway to overbill the board, receiving kickbacks from the employees of Bayway. At times, Bayway charged the board for items that were never received.

Continued on page 5

Case Studies (continued)

Utz Quality Foods False Invoice and Kickback

From January 2010 to August 2014, Utz Quality Foods, Inc., paid over $1.4 million to a vendor for products that were never actually received. The vendor, Haas Packaging & Design, was Utz's provider of packaging and shelving products. Over a 4-year period, the vendor's owner, Jonathan Haas, colluded with Utz's Director of Purchasing, Kevin Myers, to submit 83 false invoices and 43 fraudulent purchase orders. After Myers approved the false invoices for payment, he would then receive a portion of the proceeds from Haas through a false invoice kick-back scheme. Myers even created a fictional business entity, Myers Packaging Consulting, in order to conceal the kickbacks he was receiving from Haas. In the course of running the alleged false invoice scheme, Haas received approximately $1.4 million while kicking back approximately $523,500 to Myers. Jonathan Haas was convicted and sentenced to 36 months in jail and required to pay approximately $1.4 million in restitution to Utz and Utz's insurance carrier, Chubb Insurance. Kevin Myers was also convicted and sentenced to 51 months in prison.

$100 Million Business Email Compromise

In 2013, Evaldas Rimasauskas began his alleged $100 million business email compromise scheme by registering and incorporating a company in Latvia. Rimasauskas "coincidentally" gave his new company the same name as a legitimate computer hardware manufacturer in Asia, Quanta Computer, which regularly conducted multimillion dollar transactions with U.S. internet companies. Under this name, Rimasauskas created email accounts that resembled those of the computer hardware vendor. He then sent messages to employees at two large Internet companies, requesting them to wire payments for legitimate goods to a bank account under his control. The employees, believing they were communicating with one of their trusted suppliers, directed the payments to Rimasauskas' company in Latvia, instead of the true vendor, Quanta Computer. Rimasauskas was charged with one count of wire fraud, three counts of money laundering, and one count of aggravated identity theft and faced a maximum sentence of over 60 years in prison.

How to Detect and Prevent Vendor Fraud

Internal controls are a necessity for a business to mitigate the risk of vendor fraud. However, despite the importance of internal controls, controls alone are not sufficient to eliminate the risk of vendor fraud entirely. Internal controls are a well-known function in organizations to help prevent all types of fraud, and thieves and perpetrators can, and will, view internal controls as an obstacle to overcome in order to successfully defraud an organization. This does not mean an entity should take internal controls lightly.

Perform the necessary due diligence when selecting new vendors. This is an extremely important step in combating vendor fraud. Thorough background checks into a vendor's business reputation, financial stability, and overall experience are crucial. Additionally, simple checks are easy and can help to eliminate fictitious vendors. The following are some examples:

- Compare a vendor's address to the employee address master list.
- Check the address given by the vendor to confirm that it actually exists.
- Make sure the vendor has an address that would make sense based on the vendor's size and services (that is, an actual business location versus a P.O. box).
- Verify the vendor's business registration, tax ID numbers, and phone numbers.
- Conduct a cross-search through an organization's vendor database to confirm that a new vendor is, in fact, a unique new vendor and not a variation of an existing vendor in the database.

Strong internal controls around vendor master lists and the creation of new vendors can help mitigate the risk of vendor fraud.

Use separation of employee duties as a preventive internal control. Although it may seem like a basic practice for an organization when it comes to preventing vendor fraud, many companies still do not assign separate employees to separate duties as part of their internal controls.

Continued on page 6

- Separate employees should be involved in approving a new third-party vendor and inputting the new vendor into the vendor master list in order to avoid falling victim to fictitious vendors.
- Different employees should input new vendors into the vendor master list, process invoices from vendors, and process payments to vendors.
- There should be a clear separation between the employee responsible for processing vendor payments and those employees that reconcile the bank statements and accounts.
- If a company is too small to separate each of these functions individually, a careful review and monitoring of the duties discussed previously must be done by the manager or owner to help ensure proper vendors and proper amounts are paid.

Simply by segregating these tasks to various employees in the respective departments, an organization's ability to prevent vendor fraud can be greatly increased.

Use state-of-the-art detection methods. Advances in technology have made data mining easier and more cost effective as a defense against vendor fraud. Organizations can perform a variety of different data-related payment tests to identify anomalous transactions that may indicate fraud. These types of tests include the following:

- Running various queries and reports on the vendor payments made, vendor invoices received, and vendor information changes (for example, new address, new payee information), looking for multiple invoices paid on the same day to the same or related vendor, use of the same purchase order multiple times, and use of the same invoice or sequential invoice numbers
- Testing contract terms against invoices received from a specific vendor, for example, an organization can test to see if the total payments made to a specific vendor exceed the contractual limit
- Testing for duplicate payments, looking for payments made two or more times for the same invoice work performed
- Testing for payments made outside of normal business operating times, such as weekends, holidays, or late at night

Continued on page 7

ADDITIONAL PRACTICE TIPS FOR PRACTITIONERS

The following are some helpful tips for practitioners to assist clients in gaining a better understanding of vendor fraud schemes and to reduce an organization's susceptibility to such fraud:

- Provide information on how vendor fraudsters operate and the internal control weaknesses that are exploited by such thieves to perpetrate vendor fraud.
- Deliver training on technological safeguards that are available to combat against the cyber component of vendor fraud schemes.
- Assist with implementation of continuous monitoring of employee behavior, financial data, and current internal controls to help identify fraudulent activities in real time.
- Offer employee training on recognizing suspicious email requests, such as requests for electronic transfers of funds, even when the email appears to come from a reliable source, like a long-standing vendor.
- Help with development of procedures to verify the origin of wire requests. (See the AICPA fraud report on Executive Information.)

These are only a few examples of testing that can be done to help detect vendor fraud. An organization should tailor its detection program to its individual needs, including industry practices, vendor profile, and company size.

Provide anti-fraud training to all employees. Training is a critical tactic in the battle against vendor fraud. It increases employee awareness of the various vendor fraud schemes and the potential red flags that accompany those schemes.

Establish a fraud hotline. This allows an organization's employees to anonymously report any suspicious activity or irregularities without the fear of repercussions. By creating an environment that encourages employees to be vigilant when it comes to awareness of any type of fraudulent activity, an organization can greatly reduce its risk of catastrophic results from fraud schemes. Businesses should also consider the costs and benefits of providing access to the hotline externally because this would allow vendors and other third parties the ability to report suspicions. The function of operating a fraud hotline can be outsourced to a third party; however, an organization must then have established protocols to effectively follow up and resolve tips received.

Constantly review and update internal controls. Criminals who are perpetrating fraud are likely aware of the various controls in place. Thieves and fraudsters can, and will, view internal controls as an obstacle to overcome in order to successfully defraud an organization. Organizations need to understand this challenge and accept it. It is imperative that organizations ensure that internal control procedures and segregation of duties are implemented and followed. Organizations should periodically assess the success of their current controls and evaluate if additional controls and procedures should be implemented to better reduce the risk of vendor fraud. They should perform periodic risk assessments and identify the specific internal control weaknesses within their organization that create a soft target for vendor fraud. Organizations that continually test, update, and improve their internal controls will find that they can be effective in mitigating the risk of fraud.

What to Do When Fraud Is Discovered

Despite strong internal controls and procedures, it is impossible to entirely eliminate the risk for fraud within an organization. Many times, fraud is discovered simply by accident. When this happens, organizations often need to quickly get a handle on the breadth and depth of the fraud. Forensic accountants have experience and are trained to perform in-depth investigations in a time-sensitive manner while preserving evidence and records. This is critical because litigation, be it criminal or civil, or both, often follows the discovery of fraud.