Integrated Payables

Understanding the Threat of Fraud and How to Prevent it

UMB Integrated Payables UMB.com/IntegratedPayables

UMB

Understanding the Threat of Fraud and How to Prevent It

The sad reality is that most companies are targets for fraud. Organizations of all sizes are put under constant strain by suspicious and fraudulent activity and often do not have the proper controls to protect themselves. The results can be extremely damaging and include massive financial and reputational losses.

Most organizations acknowledge the nature and severity of the threat of fraud. In many instances, despite recognizing those risks, new technology causes institutional blind spots, all while fraudsters become more sophisticated with the methods they use to attack weaknesses. In order to successfully stay ahead of financial crime, a comprehensive payment fraud strategy must be developed across systems, departments and payment methods.

The issue of fraud is particularly threatening to organizations who lack internal resources responsible for managing risks. Companies who operate on lower turnover are more susceptible to serious consequences should they suffer a major fraudulent incident. Financial instability caused by fraud can threaten the very existence and reputation of a business. As such, the threat needs to be taken seriously.

The level of recent payment fraud activity is of growing concern for businesses. In 2017, payment fraud hit its highest level, according to the 2018 Fraud and Controls Report, Association of Financial Professionals.

79% of companies experienced payment fraud, cyber fraud, BEC/imposter or ransomware in the past year[1]

The Origin

Payments fraud can be categorized into two sectors, internal and external. While external fraud such as social engineering and email account compromise is covered widely in the media, internal fraud including asset misappropriation and insider fraud is rarely acknowledged. This is can be problematic, as internal fraud makes up a disproportionate percentage of the losses incurred by overall corporate fraud.

Many companies overlook this risk and fail to consider the threat their own employees pose to economic security. This may be in part due to confidence in the systems in place and a reluctance to suspect internal staff.

Regardless of whether the fraud being perpetrated internally or externally, put yourself in the shoes of a fraudster. How would you take advantage of the systems in place? What vulnerabilities would you exploit? The best way to weed out a fraudster is to think like a fraudster. Companies always benefit when they improve their controls around systems and processes, and ensure their people are in an ongoing anti-fraud mindset.

52% of fraud is committed by internal actors[2]

The Deception

For businesses, there are many types of fraud threats to consider. Four types of fraud have grown to pose a significant threat.

1. **Asset Misappropriation** is the most common type of fraud, where an employee steals cash or other assets through deceitful means. According to the Association of Certified Fraud Examiners (ACFE), more than 89% of all internal fraud schemes involved an asset misappropriation element, and the median loss from an asset misappropriation was $114,000. Asset misappropriations are commonly detected through employee monitoring or through internal controls like segregation of duties, account reconciliation, and independent verification of data.

2. **Business Email Compromise/Email Account Compromise (BEC/EAC)** is a growing problem and a critical vulnerability in many organizations. Through methods such as phishing in its many variations, social engineering, email spoofing, and malware, including vendors, billing systems, and email traffic - with the ultimate goal of deceptively impersonating and communicating with customers or internal employees to reroute payments to a fraudulent account or to steal private information for financial gain. A variation of BEC is “whaling,” which is different from basic BEC because a CEO’s email is compromised.

   The reason the number of attacks and the resulting costs are skyrocketing is simple: Attackers – whether inside or outside your institution – are using more sophisticated techniques to gain access to sensitive information. There are lucrative potential gains from a successful attack, all while the fraudster is able to maintain a great deal of distance between the crime scene and themselves. In order to protect both corporate and customer data, compliance, security, and fraud professionals must consistently rethink how they approach payment fraud detection and overall cybersecurity.

   Monitoring, profiling, analyzing, and reacting to all user behavior in real-time is just as important as building security layers to guard against outside threats.

3 Keys to Stopping BEC and EAC

- Implement Multi Factor Authentication as a best practice and establish check and balance procedures for payments and sensitive information requests
- Train employees to question and escalate suspicious emails before clicking links, downloading files, or replying
- Be on the lookout for internal requests that are unusual and often pressing for payments or data exports outside of normal procedures

3. **Social Engineering** is simply using deception, manipulation, and trickery to influence a target to perform a task or divulge information for nefarious purposes by a fraudster. Fraudsters can ask a user to give up a password, to change banking information, or to send a confidential business file because it was recently "lost" by accident. The list of potential requests can seem endless. The medium used to begin the deception can include multiple communication channels, including in person, by email, in a text, via an app, on social media or over the phone.

   With minimal access to one employee's account, fraudsters may secretly install malicious software that will give them even more access to passwords and bank information.

   Fraudsters use social engineering tactics because it is usually easier to exploit your natural inclination to trust than it is to discover ways to hack your software.

5 Ways to Protect against Social Engineering:

Maintain strong email, virus protection, and overall IT security protections.

- Set your operating system to update automatically
- Use an anti-phishing tool offered by your web browser or third party to alert you to risks
- Educate and train employees to identify red flags such as pressure, urgency, and non-standard communications and then escalate for additional review before approving, changing, or sending anything
- Establish procedures giving employees a known "way out" so they can always halt an uncomfortable conversation or raise red flags
- Verify the identity of the person you are talking with. When in doubt, communicate with the purported individual on your terms; email them something if they want to use the phone, or ask them to verify something you know would only be known to them, such as an invoice number

72%

of corporate respondents report the incidence of business email fraud. Not surprisingly, as the threat levels increase, so does the cost. 53% of victims recover nothing and 32% only make a partial recovery. Additionally, the more victims lost, the less likely they are to make a full recovery.[3]

4. **Insider Fraud** relies on accessing your valuable digital resources. However, you need to know who they are, what they're doing, and if resources have been compromised. The Fraud Triangle is a model that can explain the factors that cause a person to commit fraud:

   1. Perceived financial need or stressor
   2. Opportunities to execute the fraud (authority, access and business knowledge)
   3. Rationalization that enables the person to reconcile the situation within their own mind or values (i.e. thinking the person is really just borrowing money for a short time)

   Organizations can use the following activities to help identify and prevent an internal threat before it escalates and triggers substantial monetary and brand damage.

   - Monitor internal user activity across all systems: It is critical to establish normal and abnormal organizational benchmarks for employee activity to identify inconsistencies in behavior patterns
   - Track behavior in real time: Rather than analyze data retroactively, organizations can monitor and alert from the moment data is captured

   By leveraging these measures, fraud can be discovered at an earlier stage to prevent customer data breaches and malicious attacks.

Reducing Vulnerability in Payment Processes

Regardless of the type of fraud, organizations need to conduct regular audits and institute processes like user-based permissions and separation of duties to help reduce the occurrence of internal fraud and recognize weaknesses in their payment systems. These evaluations should assess each step of the payment journey and identify any areas that have the potential to be manipulated or abused.

This type of self-evaluation is particularly important for growing companies, as it helps to proactively identify vulnerabilities that arise through expansion. In many cases, growing businesses have few security systems in place to begin with.

Regardless of the size of the organization, companies should recognize a culture of trust is not enough to protect them. Those without the proper systems in place need to introduce them sooner rather than later, or run the risk of suffering from fraudulent activity. Those systems have the power to not only reduce the risk of fraud, but also help to identify mistakes that may in fact be incurring additional costs to the business.

With regular evaluation, loopholes can be recognized and closed before they are exploited.

According to the FBI, phishing efforts have earned cybercriminals an estimated $12 BILLION through Business Email Compromise.

27%

of companies test their own employees with fake phishing emails[1]

Taking Action

Left unchecked, fraud has the potential to cause significant damage to your business.

To minimize the risk of fraud in your organization, you need an infrastructure that coordinates your people, processes and technology to recognize and detect vulnerabilities before they are exploited.

With a well-managed fraud prevention strategy, you can radically limit fraudulent activity throughout your business and reduce the potential losses incurred. To ignore the threat of fraud is not an option, as businesses cannot afford the costs to their bottom line or their reputation that fraud incurs in today's payment ecosystem.

To learn more about UMB Integrated Payables, visit **UMB.com/IntegratedPayables**

86%

of organizations report experiencing security incidents and information theft and loss in the past 12 months[4]

Sources:

1. 2019 Treasury Fraud & Controls Survey
2. PwC's 2018 Global Economic Crime and Fraud Survey
3. ACFE 2018 Global Study on Occupational Fraud and Abuse
4. Kroll Global Fraud & Risk Report 2017/2018