Goldman Sachs | TRANSACTION BANKING

The Evolving Landscape of Corporate Payments Fraud

Introduction

Fraud is both an ever-present and a growing risk. In terms of ubiquity, more than four out of five companies (81%) said they were the target of payments fraud in 2019, according to a survey by the Association for Financial Professionals.[1] And, the threat isn't abating: 73% of organizations think that the threat level of fraud has increased in the past year.[2]

When it comes to fraud—specifically payment fraud and especially at a time when the persisting COVID-19 pandemic has negatively impacted cash flows—we naturally might gravitate to thinking about and focusing on the financial risk and the limited ability of companies to cover unexpected loss. But there's more. Compounding the issue of financial risk are the potential significant reputational risks and regulatory risks, which also can have a pernicious impact on future business performance.

Because of the prevalence and growing threat of fraud and its potential effects, businesses should recognize how fraud is evolving—and how they can shift their defense to tackle the issue. ■

73%

of organizations think the threat level of fraud has increased in the past year.

81%

of companies said they were the target of payments fraud in 2019.

Fraud Overview

The landscapes in which most businesses operate are continually evolving, as is the underlying fraud landscape. In just the same way that businesses have been able to embrace digitalization to evolve and provide more streamlined and personalized services, fraudsters have embraced digital technology to evolve the threat that they pose to businesses and the public.

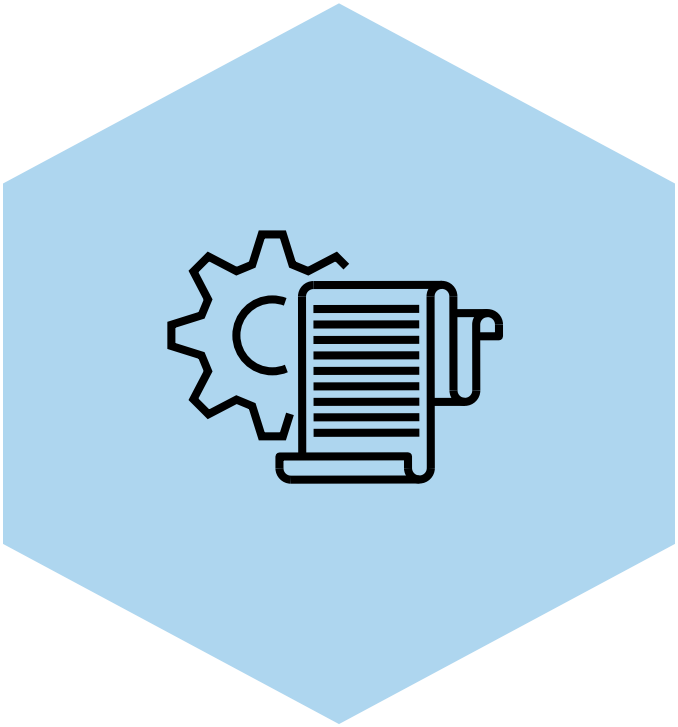
Today, the threat posed by fraudsters can be characterized by four key aspects:

- **Organization:** Fraudsters are increasingly professional in approach, even dividing their operation into different functions.
- **Complexity:** Methods of fraud-attack and the associated techniques used are increasingly sophisticated.
- **Victims:** Fraud attacks are increasingly targeted toward specific organizations and specific profiles of employees within.
- **Speed of attack:** A recurring theme for almost all corporate fraud is the aim to exfiltrate funds out of the target business as quickly as possible. External "mule" accounts are maintained to transfer funds in real time and reduce the opportunity for recovery.

The current sophistication of fraud attacks is best illustrated by a recent example of business email compromise (BEC) fraud, in which a fraudster gained access to the email account of an executive at a financial services company and imitated the account owner's identity.

The fraudster monitored emails for a two-week period before starting to send messages, culminating in a series of emails to the company's account department requesting two wire transfers totaling $10.8 million. The money was subsequently dispersed through several "mule" accounts, and only a small portion of funds could be recovered. An email inbox rule was created to hide correspondence from the compromised executive and prevent detection. ■

Business Best Practices



As fraudsters become increasingly sophisticated and organized in their approach, it is important that businesses respond equally by reviewing their own approach to the management of fraud risk. Recent research by PwC indicates that businesses with dedicated fraud programs spent 42% less than those without responding to actual fraud incidents, 17% less on remediation costs, and 16% less in fines and penalties[3].

A fundamental requirement for all businesses to manage their fraud risk is to have a fraud response plan. No matter the size or type of organization, it is increasingly becoming a case of when—not if—your business will be subject to a fraud attack.

A formal, agreed upon response plan will reduce the impact of a fraud attack. Ideally, a formal response plan may include a step-by-step process for communication, recovery of any losses, and for returning the business back to a normal state while protecting from any recurrences. The recovery plan should consider interaction with all key stakeholders, employees, customers, banking partner(s), legal advisors, and regulatory authorities.

A fraud response plan is an example of the defensive or reactive approach that businesses have traditionally used to manage fraud risk. Additional, proactive measures can be implemented to prevent fraud before it can manifest. ■

Recent research indicates that businesses with dedicated fraud programs spent 42% less than those without responding to actual fraud incidents.

Risk Assessment

Risk assessment is important, as different areas of the business will be susceptible to different levels and types of fraud attack. An example of this is the difference in underlying risk between an organization's accounts payable and accounts receivable functions. A one-size-fits-all approach to fraud management runs the risk of causing excessive negative business impact.

A comprehensive assessment will look at potential fraud risks, their likelihood of occurrence, and their potential ramifications. Any controls to mitigate fraud should also be included. A fraud risk assessment, completed on a regular basis, will provide a business with the understanding to tailor a fraud program to prevent fraud while supporting the business in its growth. All areas involved in the flow of monetary funds should be included in an assessment at a minimum, if not the entire organization.

Risk assessment also provides the ability to assess one of the fundamental principles of fraud risk management: segregation of duties. This is a basic fraud mitigation element that almost all organizations will have implemented. In an ever-evolving business environment, however, new processes and technology can alter roles and responsibilities, and potentially circumvent previously segregated duties. A regular fraud risk assessment ensures that segregation is still valid and proactively highlights the need for any change. ■

Risk assessment also provides the ability to assess one of the fundamental principles of fraud risk management: segregation of duties.

Technology

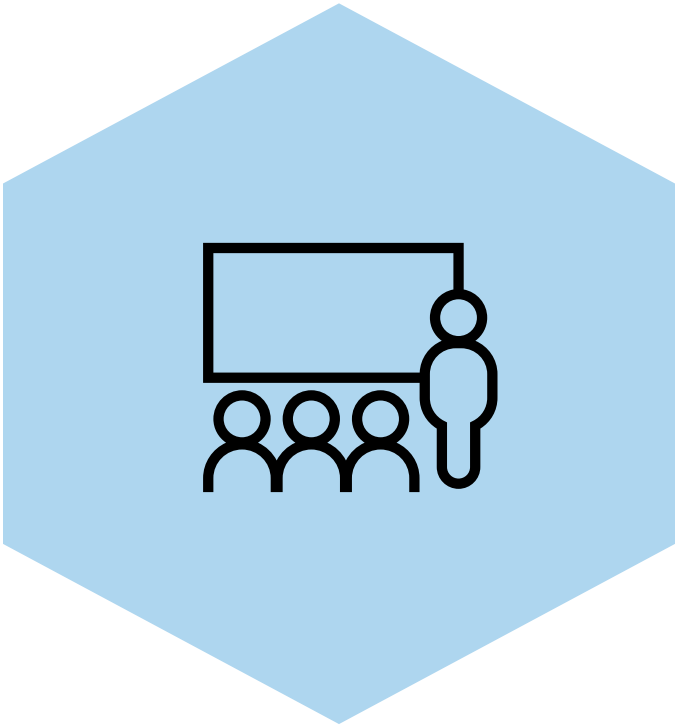
Technology usage is a key lever for managing fraud risk. Technology solutions implemented within the organization can provide support in monitoring for anomalies in your business activity that could be indicative of fraud, at all levels.

Solutions may include machine learning to process and generate a decision from potentially millions of pieces of data in a time frame that would not be feasible for traditional, manual in-house approaches. Adopting a multilayer strategy where both the organization and the banking partner deploy monitoring and detection technology maximizes the ability to manage fraud risk and reduce negative impact on genuine payments. However, it is not just detection where technology can be leveraged. Technology can be used to automate certain processes within your business and therefore reduce the scope of human involvement in that process and equally reduce the scope for process abuse or compromise.

In an era when fraudsters are actively searching for and harvesting access credentials, adding additional levels of authentication technology, or multifactor authentication, to processes can be an effective deterrent to the takeover of systems. Biometric multifactor authentication is an effective technology solution that provides an authentication source that is very difficult for an external fraudster to compromise, while minimizing the impact of additional authentication layers for employees. ■

Adopting a multilayer strategy maximizes the ability to manage fraud risk and reduce negative impact on genuine payments.

Employee Training



Though technology plays an increasingly important role in fraud controls and detection, it can be manipulated and overridden. The importance of human involvement in the fraud management process remains central for oversight of technology solutions and for detecting fraud.

It is important that all employees involved understand their role in the controls. It is likely that a blend of technological and human involvement will be considered the optimal solution for managing fraud for the foreseeable future.

With employees retaining an important involvement in the fraud management process, the importance of fraud awareness training remains critical for all organizations. Fraud awareness training ensures employees are educated on fraud risks, specific fraud types, and the red flags to identify them. To be effective, training needs to be continuous from point of hire onward. For employees in areas assessed to be high-risk, advanced training of fraud and testing of understanding will ensure that these employees are cognizant of the increased risks. Fraud awareness also serves to protect the business from experiencing negative impact from social engineering schemes.

Fraud awareness training is an important process for preventing and detecting fraud; however, compliance training is also critical for insider-fraud risk to communicate standards on organizational culture, and to communicate internal policies on conduct and prohibited actions.

To further combat the risk of insider fraud, a user-monitoring program can be an effective method of identifying suspicious behavior. A program can take the form of a software solution that can provide real-time monitoring and alerting of any suspicious activities, or an offline analytics solution using the audit logs of your business systems. Suspicious behaviors include employees logging on at unusual times or with unusual frequency, or attempting to access systems that are not applicable for their role. ■

The Role of the Banking Partner

Products and services offered by your banking partner should have been designed with a risk-assessment approach to make them as secure as possible.

Examples of risk-assessed products include those employing multifactor authentication at payment initiation and make/checker requirement at payment initiation. Features like "positive pay" allow filtered exceptions to pass through an additional review and decision by appropriate levels of users within the customer organization.

In the event of a fraud attack, the banking partner should be able to assist with attempting a recovery of funds associated with a fraud and by restricting access to banking applications as needed.

Conclusion

The corporate payment fraud landscape is increasingly sophisticated, and organizations need to deploy a dedicated fraud program to proactively assess and implement appropriate fraud controls. Employees continue to be an important part of a fraud program, and organizations need to ensure sufficient training is delivered to leverage the capability of employees in detecting fraud and limiting losses. ■

[1] *2020 Fraud and Control Survey,* Association of Fraud Professionals. |
[2] *2019 Treasury Fraud and Controls Survey Report,* Strategic Treasurer |
[3] *2020 Global Economic Crime and Fraud Survey,* PwC