Portfolio Media. Inc. | 111 West 19th Street, 5th Floor | New York, NY 10011 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

Compliance Solutions For Pandemic-Related Fraud Risks

By **Matt Rutter and Rachel Berk** (July 1, 2021, 2:32 PM EDT)

Matt Rutter

Rachel Berk

When the COVID-19 pandemic struck the U.S. in March 2020, office environments, supply chains and traditional ways of doing business evaporated in mere weeks. Many organizations were forced to alter their processes to adapt to a quickly changing environment or risk their business operations failing.

Ultimately, business continuity took precedence so that organizations could continue to operate as business as usual, and therefore, risk-remediating controls may have been sidelined. And in many instances, boot-strapped solutions proliferated as companies quickly modified processes to reflect new business realities.

As organizations now prepare to head back into the office and embark on post-pandemic business operations, individuals charged with governance should consider whether their anti-fraud compliance programs are robust enough to handle the additional risks posed by the pandemic, and whether their overall risk and compliance framework is ready to emerge from the pandemic stronger.

We consider relevant risks and accompanying solutions for you to contemplate as the pandemic subsides and companies contemplate their next move.

Vendor Fraud, Kickbacks and Corruption

Vendor disruption is a headline risk as companies continue to operate in a virtual environment with hybrid workforces. And with supply chains disrupted, many third-party relationships were initiated, modified or terminated.

It is easy to imagine a scenario where a critical vendor went offline due to COVID-related issues, and instead of engaging in a formal bidding process as is customary in order to identify and engage a new vendor, the organization scrapped its bidding process in favor of an expedited selection process that promoted business continuity.

Although this expedited solution yielded a possible near-term win for the company, several issues could arise down the road if a vendor was not properly vetted during the onboarding process, such as undisclosed related party transactions resulting in collusion and kickbacks.

Organizations should also assess one-time payments to vendors, such as those classified as COVID-related expenses, gifts, sponsorships or charitable contributions that could be indicative of bribery or corruption.

Additionally, cyber threats related to social engineering, spoofing, and phishing schemes are on the rise.[1] Combining the disruption of 2020 with these rising cyber risks cited by the U.S. Securities and Exchange Commission, companies are even more vulnerable to predatory behavior and violations.

For example, assume an accounts payable clerk receives an email from a purported client manager representing a key vendor, who claims that the former point of contact has left the vendor as a result of the pandemic and thus, they are writing to inform of revised payment instructions for outstanding invoices.

In this scenario, it is critical for an organization to first socialize this information internally and then verify the authenticity of the message before issuing any further payments to the vendor.

Organizations can protect against bribery, social engineering, vendor collusion and similar payment-related schemes by building awareness of known schemes and existing controls, and further, by fortifying the firewall of existing controls with the design and implementation of new controls.

Below are several examples of risk-mitigating activities that companies can implement:

- Emphasize that payment requests, regardless of their extraordinary nature, follow appropriate approval protocols and escalations.

- Encourage employees to consult internally with peers or supervisors if presented with an unexpected or unusual vendor request or communication.

- Notify employees through regular communications or training to be aware of potential spoofing or vendor-related schemes.

- Require that changes to vendor payment details and points of contact be contractually agreed-to terms, and require authorization from each party to the agreement.

- Conduct due diligence during vendor selection and onboarding process, and continuously monitor vendors and contract terms.

- Perform transaction testing for high-risk areas such as gifts, sponsorships and charitable contributions.

Attrition and Eroding Compliance Culture

Culture is often cited as the special sauce that drives organizational success. For many organizations, the disruption of 2020 into 2021 has presented unique challenges, and several executives have voiced concern that corporate culture was eroding during the pandemic.

Embedding culture is more challenging when the workforce is physically dispersed, organic interactions are limited, companies have lost key personnel either due to natural attrition or layoffs, or cost centers

such as compliance have been trimmed or deprioritized.

A weaker corporate culture could lead to an environment where the risk of employee fraud or misconduct is more likely. As Gallup Research scientist Jim Harter told Harvard Business Review, "Engaged employees are more attentive and vigilant."[2] And employee engagement is often fostered by a cohesive corporate culture.

Further, employees working remotely may inappropriately deem themselves to be more autonomous with less supervision and therefore take additional risks not otherwise considered.

According to data by NAVEX Global Inc., a third-party manager of whistleblower hotlines, reports to corporate ethics hotlines dropped roughly 7.1% in 2020 from the preceding year.[3]

While one year alone does not make a trend, this statistic is a helpful reminder that whistleblower programs are successful in large part due to awareness. With employees out of the office, as has been the case throughout 2020 and 2021, those whistleblower hotline notices in the copy room, kitchenette and common rooms have less visibility, and thus, employees may be hesitant to report potential wrongdoing.

As organizations plan for return-to-office operations, individuals charged with governance should evaluate their current environment and determine whether their culture of anti-fraud compliance has receded and, as a result, their ability to prevent, detect, investigate and remediate fraud or other irregularities efficiently and effectively has been impacted.

In those instances, organizations should consider conducting a companywide risk assessment to further identify and assess fraud-related risks that may have arisen during or as a result of the pandemic. These engagement-building exercises solicit feedback from employees on the myriad risks that are on their radar, the likelihood of those risks occurring and potential impacts if those risks are realized.

Once risks are identified and mitigating controls are identified or added, organizations can then roll out specific measures, such as conducting transaction testing on newly identified fraud risk areas, or targeted communications, surveys, outreach programs and continuous training, to strengthen their mission, tone and anti-fraud compliance culture that may have languished or been impacted during the peak and aftereffects of the pandemic.

Financial Reporting Fraud

During the past year, revenue, earnings per share and margin came under intense pressure as many organizations made operational changes, sometimes in haste, to the meet the challenges born by the pandemic.

In addition, metrics in 2020, 2021 and 2022 will fluctuate wildly when compared on a quarterly and annual basis, so assessing the reasonableness of metrics and whether they are fairly presented will be difficult.

Revenue-related fraud was the most frequently occurring type of reporting fraud prior to the pandemic and will remain an outsize fraud risk as the pandemic subsides.[4][5]

As customers potentially face cash flow stress and agreements may be modified, organizations must

consider how contractual concessions may impact whether a company can recognize revenue and what amount should be recognized.

Further, the pandemic has redefined when performance obligations are considered fulfilled, and as an extension, when revenue based on those obligations may be recognized.

Similarly, organizations can inappropriately capitalize expenses to stretch the impact to the bottom line over subsequent quarters and years. During the pandemic, many organizations invested in business continuity and in turn, may have created assets yielding significant future value.

With the pandemic's impact waning, organizations should now assess whether a future benefit remains or whether they should write down such assets.

The use of data analytics is a potential antidote to such financial reporting challenges.

Analytics can serve as an early warning system, identifying issues in a targeted fashion, thus allowing organizations to avoid rushed or, worse, retrospective or costly assessments of potential reporting requirements.

A good first step is for an organization to assess what data does or does not exist and how data is shared across different platforms within the organization to determine what insights can be gleaned from the available data sources.

The amount of available data and the design of a company's system of databases inform the types of analyses that can be performed and the level of early detection that can be achieved.

Given the increased use of and focus on data analytics by the U.S. Department of Justice, it is critical for organizations to assess their own access to data in order to identify, monitor and prevent any potential financial reporting issues or areas of misconduct.

As part of the DOJ's 2020 update to its guidance on corporate compliance programs, the department included specific references to the use of data analytics and emphasized the importance of sufficient access to relevant sources of data for compliance personnel.

As businesses emerge from the pandemic and resume operations resembling pre-COVID conditions, it is critical for those charged with governance to consider any pandemic-related risks that emerged during 2020 into 2021 and respond accordingly, whether that means revisiting vendor contracts and terms that were established during the pandemic, conducting a companywide risk assessment to identify and remediate relevant or new fraud risks, or using data analytics for the purpose of identifying potential financial reporting frauds or trends.

Matt Rutter and Rachel Berk are principals at Charles River Associates.

[1] In 2018, the SEC published a Report of Investigation detailing how companies were increasingly

falling victim to "cyber-related frauds that may have violated the federal securities laws by failing to have a sufficient system of internal accounting controls."[1] Issuers are required, per Sections 13(b)(2)(B)(i) and (iii) of the Securities Exchange Act of 1934 to design, implement, and manage internal accounting controls to mediate access to company assets and authorize transactions appropriately.

[2] https://hbr.org/2013/07/employee-engagement-does-more.

[3] https://www.wsj.com/articles/reports-on-corporate-ethics-hotlines-fell-in-2020-11617615001.

[4] ACFE – Report to the Nations 2020 - https://www.acfe.com/report-to-the-nations/2020/.

[5] Accounting Standards Codification Topic 606 (ASC606) – Revenue from Contracts with Customers.