



■ **INDEPTH FEATURE** Reprint March2022

CORPORATE FRAUD & CORRUPTION

Financier Worldwide canvasses the opinions of leading professionals around the world on the latest trends in corporate fraud & corruption.





UNITED STATES

Guidehouse

Respondents



ELLEN ZIMILES

Partner

Guidehouse

+1 (212) 554 2602

ellen.zimiles@guidehouse.com

Ellen Zimiles is a partner and the firm's financial services advisory and compliance segment leader. She has more than 30 years of litigation and investigation experience involving many high-profile money laundering, fraud and forfeiture cases. Also an internationally recognised expert in anti-money laundering (AML) programme development, corporate governance, regulatory and corporate compliance, fraud control, and public corruption matters, she has worked with a multitude of financial institutions preparing for regulatory exams, developing remediation programmes, and serving as regulatory liaison.



SALVATORE LASCALA

Partner

Guidehouse

+1 (212) 554 2611

salvatore.lascala@guidehouse.com

Salvatore LaScala is a partner and head of Guidehouse's global investigations and compliance practice. Possessing a broad range of subject matter knowledge and expertise, Mr LaScala applies his 20-plus years of hands-on experience to conduct investigations and compliance reviews on behalf of financial institution clients responding to regulatory or law enforcement matters concerning anti-money laundering (AML), Bank Secrecy Act (BSA), USA PATRIOT Act and Office of Foreign Assets Control (OFAC). He also helps clients overcome AML and OFAC backlogs by deploying teams embedded at his clients' work sites to that disposition alerts.

Guidehouse

Q. To what extent are boards and senior executives in the US taking proactive steps to reduce incidences of fraud and corruption from surfacing within their company?

A. Corporate fraud and corruption are issues that have affected financial sectors tremendously, increasing in prominence in recent years. Financial institutions (FIs) tend to be particularly concerned with fraud, as it has a direct negative impact on revenue and can erode the confidence of customers. FIs work to have robust anti-fraud and anti-corruption programmes that utilise enterprisewide fraud risk assessments of existing products, businesses and channels, as well as new product offerings. While there are a variety of controls, most are focused on prevention and detection of fraud perpetrated by employees, customers and outside actors posing as customers. With increasing activity occurring online, FIs are always looking to enhance and leverage technology to match the technology used by individuals and organised fraud corruption rings. Account takeover as a typology is a primary example of this – FIs use several methods

to prevent and detect fraud, such as requiring additional authentication for logins and reviewing IP address logins for unusual activity and alerting customers of instances where their accounts may have been compromised.

Q. Have there been any significant legal and regulatory developments relevant to corporate fraud and corruption in the US over the past 12-18 months?

A. In December 2021, the White House issued the ‘United States Strategy on Countering Corruption’, pursuant to the National Security Study Memorandum-1, in which president Biden described corruption as a core national security interest. The strategy set forth five key pillars in combatting corruption to identify and seek to rectify persistent gaps in the fight against corruption. First, modernising, coordinating and resourcing US government efforts to fight corruption. Second, curbing illicit finance. Third, holding corrupt actors accountable. Fourth, preserving and strengthening multilateral anti-corruption architecture. Finally, improving diplomatic engagement and leveraging foreign assistance resources

Guidehouse

to advance anti-corruption policy goals. More generally, 2020 and 2021 saw a dramatic increase in fraud and, as a result, it has gotten heightened attention in enforcement. Some of these fraud trends were specific to the Coronavirus Aid, Relief and Economic Security Act and COVID-19, with fraudsters taking advantage of everything from government programmes to peoples' desire to protect their loved ones with unapproved or phony at-home tests and vaccines. Much of this activity has the potential to persist long after COVID-19 is gone. The Federal Trade Commission (FTC) released a report on fraud trends, stating, "Prizes, sweepstakes, and lotteries; internet services; and business and job opportunities rounded out the top-five fraud categories". The report notes that the agency received 2.8 million complaints, with losses totalling \$5.8bn in 2021.

Q. When suspicions of fraud or corruption arise within a firm, what steps should be taken to evaluate and resolve the potential problem?

A. First and foremost, suspicions of fraud need to be taken seriously and addressed

with the appropriate sensitivity. When subjects of accusations are prestigious or senior individuals in an organisation, allegations merit an even more formal approach, and it might make sense to have an outside firm handle the investigation. Perhaps Elizabeth Holmes, founder of Theranos, might have been brought to justice sooner had the firm's board of directors been better trained and had access to an independent review early on. A culture where individuals are discouraged from asking basic due diligence questions should be a red flag. Additionally, firms should initiate investigations promptly. If the allegations of wrongdoing prove to be true, there could be both financial and reputational implications in sitting on the information for too long.

Q. Do you believe companies are paying enough attention to employee awareness, such as training staff to identify and report potential fraud and misconduct?

A. Most FIs are proactively raising employee awareness in identifying, reporting and reducing potential fraud. However, FIs' understanding of fraud



Guidehouse

typologies can lag behind their invention. While employees may be trained to identify and escalate fraud, the problem most institutions face is being able to proactively identify fraud, so they are not reliant on employee interdiction. In collaboration with the American Banker, we recently conducted and released the findings of a fraud survey titled ‘Optimizing Your Anti-Fraud Technology’, which aims to uncover how FIs are building an integrated fraud programme. In response to the survey, approximately 37 percent of FIs indicated they are somewhat or not effective at addressing new and more complex threats. This might be the result of not having a continuous risk assessment process to evaluate risks from new and unforeseen threats. A similar percentage of respondents indicated that they do not have sufficient investment, adequate tools or technologies to prevent and detect fraud. More than 90 percent of FIs rely on third-party vendors for supporting ongoing maintenance, operation and governance of their anti-fraud programmes and technologies.



Most FIs are proactively raising employee awareness in identifying, reporting and reducing potential fraud. However, FIs’ understanding of fraud typologies can lag behind their invention.

Guidehouse

Q. How has the renewed focus on encouraging and protecting whistleblowers changed the way companies manage and respond to reports of potential wrongdoing?

A. Companies should be mindful about protecting, and not retaliating against, individuals coming forth with reports of potential wrongdoing. The renewed focus may have the effect of additional whistleblowers coming forward. Companies that are prepared with a governance structure in place to investigate allegations in such a way that the individual raising the concern feels protected from retaliation are less likely to be surprised by allegations in a more public forum. Companies that are growing quickly may be particularly susceptible, as they might not have the compliance infrastructure growing at the same rate as the rest of the company. Whistleblowers may also perceive their cause receives more attention in a public forum and, in the event someone raises allegations outside the organisation first, companies need to be able to respond quickly using existing protocols for internal investigations.

Q. Could you outline the main fraud and corruption risks that can emerge from third-party relationships? In your opinion, do firms pay sufficient attention to due diligence at the outset of a new business relationship?

A. Larger, more established global institutions tend to have IT and physical access controls and change management controls embedded in their infrastructure to guard against third-party frauds, and are, in fact, required to do so and required to evaluate the Foreign Corrupt Practices Act (FCPA) risk to third parties. Emerging firms likely do not have this part of third-party fraud prevention fully developed and are vulnerable to third parties that require electronic access and physical access to perform their duties. Whether or not the firm pays sufficient attention to due diligence at the outset really depends on the culture of the firm and the maturity of its anti-corruption programme.

Q. What advice can you offer to companies on implementing and maintaining a robust fraud and corruption risk management process, with appropriate internal controls?



Guidehouse

A. There are a few main staples of anti-fraud and anti-corruption risk management programmes that FIs should have as part of their framework. Institutions should conduct a fraud risk assessment to understand their susceptibility to fraud and corruption risk and use that understanding to gauge the strength of or guide the development of mitigating controls. FIs should also reassess such risks and the effectiveness of the controls annually. These controls include the development, implementation and training on policies and procedures, the use of fraud prevention and detection technology solutions, due diligence and risk assessments for third parties, standard protocols to guide internal investigations and the retaining of outside counsel, and appropriate escalation for the reporting of incidents. Depending on the size and complexity of the institution, and the data available to them, FIs should consider intelligent process automation and advanced analytics to sift through large volumes of data to identify fraud, which might otherwise go undetected. □

www.guidehouse.com

GUIDEHOUSE is a leading global provider of consulting services to the public and commercial markets with broad capabilities in management, technology and risk consulting. The firm helps clients address their toughest challenges with a focus on markets and clients facing transformational change, technology-driven innovation and significant regulatory pressure. Across a range of advisory, consulting, outsourcing, and technology and analytics services, Guidehouse helps clients create scaleable, innovative solutions that prepare them for future growth and success.

ELLEN ZIMILES Partner
+1 (212) 554 2602
ellen.zimiles@guidehouse.com

SALVATORE LASCALA Partner
+1 (212) 554 2611
salvatore.lascala@guidehouse.com

