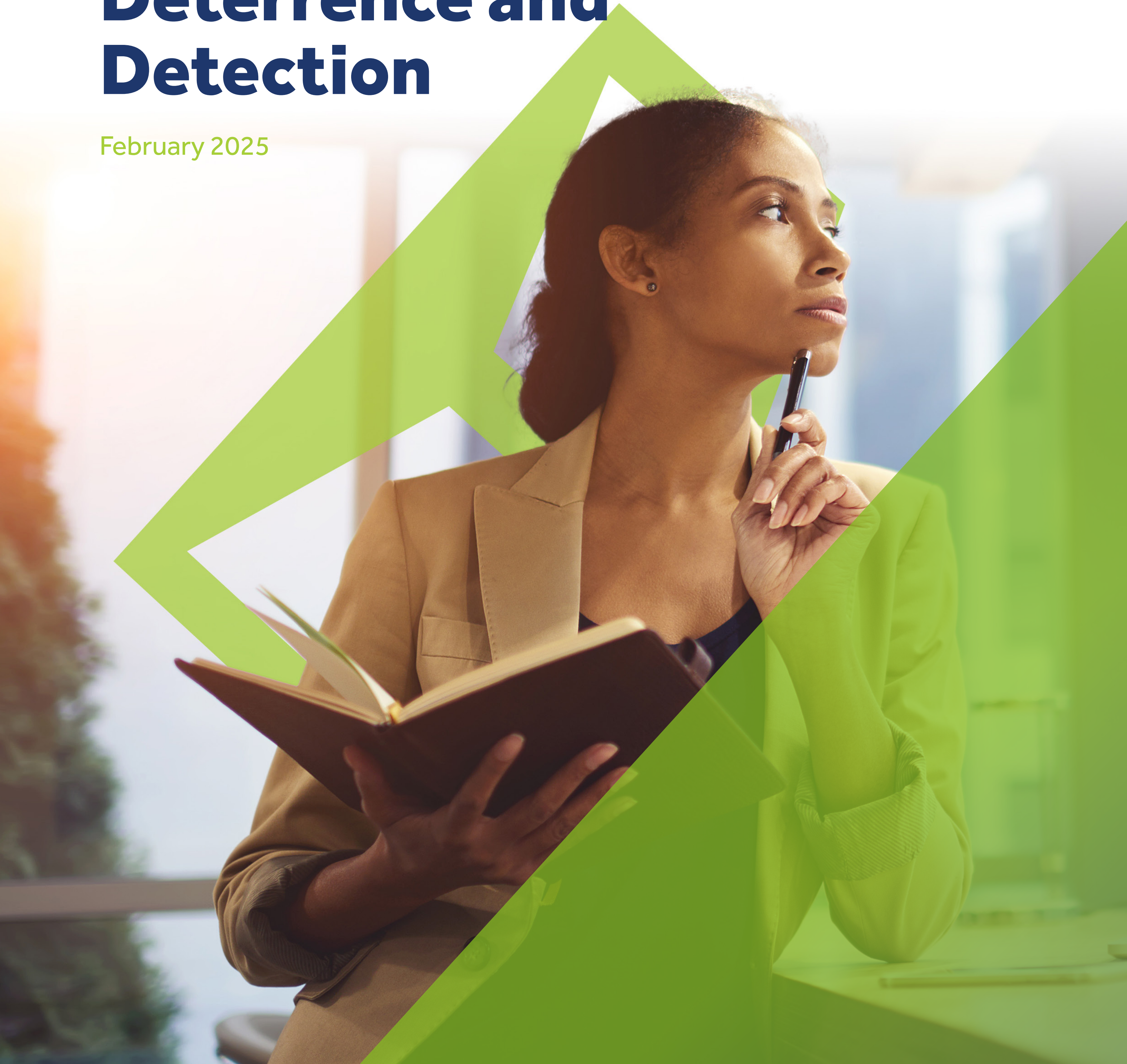
A Fraud Forum Hosted by
the Anti-Fraud Collaboration:

Continuing to Strengthen Fraud Deterrence and Detection

February 2025



About the Anti-Fraud Collaboration

The Anti-Fraud Collaboration, a partnership composed of the Center for Audit Quality (CAQ), Financial Executives International (FEI), The Institute of Internal Auditors (IIA), National Association of Corporate Directors (NACD), and Association of Certified Fraud Examiners (ACFE), is dedicated to advancing the discussion of critical anti-fraud efforts through the development of thought leadership, awareness programs, educational opportunities, and other related resources focused on enhancing the effectiveness of financial fraud risk management.

The Center for Audit Quality (CAQ) is a nonpartisan public policy organization serving as the voice of U.S. public company auditors and matters related to the audits of public companies. The CAQ promotes high-quality performance by U.S. public company auditors; convenes capital market stakeholders to advance the discussion of critical issues affecting audit quality, U.S. public company reporting, and investor trust in the capital markets; and using independent research and analyses, champions policies and standards that bolster and support the effectiveness and responsiveness of U.S. public company auditors and audits to dynamic market conditions. For more information, visit www.thecaq.org.

Financial Executives International (FEI) is the leading association and advocate for the views of corporate financial management. Its members hold policy-making positions as chief financial officers, chief accounting officers, controllers, treasurers, and tax executives at companies in every major industry. FEI enhances Member professional development through peer networking, career management services, conferences, research, and publications. Members participate in the activities of local Chapters in the U.S. FEI is located in Morristown, NJ. Visit www.financialexecutives.org for more information.

The Institute of Internal Auditors (IIA) is the internal audit profession's most widely recognized advocate, educator, and provider of standards, guidance, and certifications. Established in 1941, The IIA today has more than 200,000 members from more than 170 countries and territories. The IIA's global headquarters are located in Lake Mary, Fla. U.S.A. For more information, visit www.theiia.org or www.globaliia.org.

The National Association of Corporate Directors (NACD) empowers more than 20,000 directors to lead with confidence in the boardroom. As the recognized authority on leading boardroom practices, NACD helps boards strengthen investor trust and public confidence by ensuring that today's directors are well-prepared for tomorrow's challenges. World-class boards join NACD to elevate performance, gain foresight, and instill confidence. Fostering collaboration among directors, investors, and corporate governance stakeholders, NACD has been setting the standard for responsible board leadership for 40 years. To learn more about NACD, visit www.NACDonline.org.

The Association of Certified Fraud Examiners (ACFE) is the world's largest anti-fraud organization. By delivering best-in-class training, offering the CFE credential and fostering a dynamic, global community of anti-fraud professionals, the ACFE is reducing fraud and corruption worldwide. For more information, visit www.acfe.com.

Contents

Executive Summary

- The Center for Audit Quality (CAQ) and Anti-Fraud Collaboration (AFC) convened a multi-stakeholder dialogue amongst members of the financial reporting ecosystem at an inaugural Fraud Forum during the 2024 International Fraud Awareness Week. Participants explored the current and future state of the fraud risk landscape, discussed the prevalence of financial reporting fraud, considered existing roles and responsibilities from the perspective of their roles, and shared insights into key considerations for strengthening fraud deterrence and detection practices.
- Fraud is an inherent risk when considering the external pressures that are always present in the US capital markets, and it poses a substantial risk across all organizations. However, most participants believed that massive frauds are not pervasive across corporate America, that they have been observed less frequently in recent years, and are not thought to be likely at public companies. It is important to level set and define the type of fraud when discussing the pervasiveness and impact of fraud as not all fraud is identical, and companies do not necessarily face the same types of fraud risk, or risks at the same scale, even though the risk of fraud may be inherent.
- Fraud is generally considered a low likelihood event, but it can have a very significant impact. It was suggested that too much emphasis may be placed on the likelihood of fraud, rather than the impact of fraud, potentially preventing fraud from being detected more frequently. As the fraud risk landscape changes and evolves, so should the work of all gatekeepers (e.g., management, internal and external auditors).
- Participants emphasized the importance of considering the "human element" of fraud in fraud deterrence and detection efforts. Culture and ethics are two related and critical elements to consider when assessing and responding to fraud risks. A company can have an extremely robust compliance program on paper, but if the company's culture and values do not embrace compliance, then its programs will likely not be effective.
- Hotlines and reporting programs are an area to which financial reporting stakeholders can pay more attention for purposes of informing their fraud-related procedures. In addition to assessing a hotline for its effectiveness, using the data that is collected from the hotline is also important as it can reveal a trove of valuable information, regarding the company's culture and trust in using the hotlines in addition to potential indicators of fraud.
- Overall, the financial reporting landscape is becoming more complex and the ways through which fraud is committed in the future could be very different from what they are today. Therefore, it is important for management and internal auditors as well as external auditors to identify the fraud risks and add fresh perspectives every year during fraud-related audit procedures. There was a general consensus that standards and principles can only go so far in the fight against fraud due to the "human element" of both the perpetration and detection of fraud.
- Remaining vigilant, including exercising professional skepticism and having a questioning mind, remains vitally important for every member within the financial reporting ecosystem in the fight against fraud. As financial reporting fraud continues to be at the forefront of the public interest, finding the balance between standards, regulations, and investor protection is important to the durability and attractiveness of our US public markets.

Overall, the financial reporting landscape is becoming more complex and the ways through which fraud is committed in the future could be very different from what they are today.

Introduction

BACKGROUND

In response to the changing regulatory environment and increased focus on fraud, particularly the auditor's responsibilities related to fraud, the Center for Audit Quality (CAQ) and Anti-Fraud Collaboration (AFC) hosted an inaugural in-person Fraud Forum during the 2024 International Fraud Awareness Week in Washington, DC.

The Fraud Forum convened a multi-stakeholder dialogue amongst members of the financial reporting ecosystem, including external auditors, internal auditors, preparers and financial management, boards and audit committees, forensic experts and anti-fraud professionals, compliance and risk officers, investors, and regulators (see **Appendix** for a listing of participants and observers).

The Fraud Forum covered four key topical areas:

- The current financial reporting fraud risk environment
- Investor perspectives on financial reporting fraud and the role of each stakeholder group in deterring and detecting fraud
- Existing practices on fraud deterrence and detection by each key stakeholder group
- Practices to strengthen fraud deterrence and detection across the financial reporting ecosystem, including developing and assessing hotline and reporting programs

Participants explored the current and future state of the fraud risk landscape, discussed the prevalence of financial reporting fraud, considered existing roles and responsibilities from the perspective of their roles, and shared key considerations for strengthening fraud deterrence and detection practices, including culture, skepticism, internal controls, adopting new accounting standards, and the impact of changing regulatory requirements focused on fraud.

INTENDED USE AND AUDIENCE

For purposes of the Fraud Forum and exploring the impact of fraud on US public companies, the discussions centered on financial reporting fraud and misappropriation of assets. Participants noted the importance of considering other types of fraud as well, including occupational fraud, bribery and corruption, and others, in order to effectively assess and respond to the various fraud risks that may be unique to each organization.

This report summarizes key takeaways from the series of panels and roundtable discussion at the Fraud Forum. The summary is intended for all members of the financial reporting ecosystem and other relevant key stakeholders, all of whom have a role in deterring and/or detecting financial reporting fraud. The insights, practices, and recommendations discussed herein are based on the participants' experiences and their own views only. The information in this report is not intended to be complete or definitive, as key points from each session have been paraphrased and synopsized for brevity.

Participants explored the current and future state of the fraud risk landscape and shared key considerations for strengthening fraud detection and deterrence practices.

Current Fraud Risk Landscape

A panel of experts explored the current fraud risk landscape at US public companies, including the prevalence of financial reporting fraud today and emerging risks that need to be taken into consideration for the future. Financial reporting fraud can be defined as intentional misstatements or omissions of amounts or disclosures in financial statements designed to deceive financial statement users (see PCAOB AS 2401: *Consideration of Fraud in a Financial Statement Audit*). In response to the discussion, participants explored the challenges related to fraud deterrence and detection and the priorities in consideration of the current fraud risk landscape for public companies and regulators.

THE PREVALENCE OF FINANCIAL REPORTING FRAUD

Fraud is an inherent risk when considering the external pressures that are always present in the US capital markets, and it still poses a substantial risk across all organizations. However, most participants believed that massive frauds are not pervasive across corporate America, that they have been observed less frequently in recent years, and are not thought to be likely at public companies due to changes made by the Sarbanes-Oxley Act (SOX) for management, auditors, and audit committees.

According to the ACFE's Occupational Fraud 2024: A Report to the Nations, a global study of real fraud cases that examines the scale and impact of fraud across every type of organization, far fewer fraud cases were reported for US public companies compared to the total population of cases submitted (161 of 1,760 or 8% of cases were specific to US public companies). ACFE's study found that public companies have more anti-fraud controls in place compared to other organizations, with the following controls being most common:

- Code of conduct
- Management certification of financial statements
- Internal audit department
- Hotline

Given the maturity of public companies and the regulatory environment in which they operate, public companies are detecting fraud sooner and before it becomes as sizeable as it may compared to other types of organizations (e.g., private, non-profit, governmental). Participants were reminded that it is important to level set and define the type of fraud when discussing the pervasiveness and impact of fraud as not all fraud is identical, and companies do not necessarily face the same types of fraud risk, or risks at the same scale, even though the risk of fraud may be inherent.

Given the maturity of public companies and the regulatory environment in which they operate, public companies are detecting fraud sooner and before it becomes as sizeable as it may compared to other types of organizations.

EMERGING FRAUD RISKS AND CONTRIBUTING FACTORS

The convergence of the conditions that are commonly known as the fraud triangle—pressure/incentives, opportunity, and rationalization—tends to lead individuals to commit fraud. Those conditions can be exacerbated by both intrinsic and extrinsic factors. Legal and forensic experts discussed some of the emerging factors that may impact fraud risk in the current environment, including:

- Geopolitical risks
- Sanctions and export controls
- Third parties
- Corporate culture
- Talent pipeline

Geopolitical risks, sanctions and export controls: As the fraud risk landscape is continually changing, the risks of fraud are also changing. Geopolitical risks have a significant impact on fraud risks (e.g., ongoing wars, political unrest). Businesses operating in jurisdictions affected by such events will likely face heightened risks. Other factors such as sanctions and export controls are also ever-evolving areas of risk to which companies should be paying attention. Fraud is usually a culmination of several factors from more than one place, and given the complexities of the changing landscape, companies should approach these risks with a holistic perspective rather than assessing and responding to them in silos.

Third party risks: Fraud committed by third parties remains a major risk factor, especially for multinational companies that have operations in multiple jurisdictions. Any time a company turns over a part of its business to a third party it can create risk, particularly from a bribery and corruption perspective if those third parties are interacting with government officials internationally. An effective practice to mitigate third party risk is to conduct appropriate due diligence prior to engaging a third party and to continue to monitor the third parties throughout the course of the relationship as the risks and relationships may change over time.

Corporate culture: Fraud is not an accounting problem, it's a human problem. People commit fraud for a myriad of reasons such as financial gain, loyalty to the company, lack of knowledge, and the lack of an obvious victim. Due to the human element of fraud, it can be very difficult to detect fraud when there is collusion, especially if senior management is involved. As such, one of the most significant factors affecting the risk of fraud at any company is its culture. Participants emphasized the importance of reinforcing a strong ethical culture at every level of a company—from tone at the top, mood in the middle, to buzz at the bottom (or beginning). This includes holding people, including management, accountable if something occurs outside the norm of the company's culture.

Talent pipeline: When considering the future fraud risk landscape, one of the potential threats to combatting fraud is the challenge surrounding the accounting and auditing profession's talent pipeline. Correlations among pressure, burnout, and fraud were discussed as contributing factors for an increasing scarcity of students choosing to enter the profession. Thus, it becomes even more important to discuss what the auditor's role is, and is not, related to fraud detection. There is an opportunity for leaders in the profession to offer support to those entering the profession, and those at mid-level, to bolster the future pipeline and to retain existing talent.

BIG IDEA

Companies can move towards a more holistic and intentional effort with their anti-fraud programs by breaking up the silos and assigning ownership of fraud at the C-suite level, such as creating a Chief Fraud Officer role or elevating the role of the Chief Compliance Officer to emphasize the importance of deterring and detecting fraud.

BIG IDEA

Companies need to be able to effectively harness the enormous amount of data that they have. A company's compliance and internal audit functions need to have access to the same data that the business does in order for its compliance and internal audit programs to be effective.

Current State of Fraud Deterrence and Detection

The Fraud Forum presented a series of panels featuring a diverse group of subject matter experts, including investors, compliance and risk officers, and members of the financial reporting ecosystem (i.e., internal and external auditors, audit committee members, preparers). The panelists explored a broad range of topics relating to the current state of fraud deterrence and detection including:

- Investor expectations for different stakeholder groups' roles and responsibilities related to fraud detection and fraud risk mitigation
- Investor perspectives on emerging fraud-related issues in light of the current fraud risk environment
- Current roles and responsibilities of each stakeholder group within the financial reporting ecosystem related to fraud detection and/or fraud risk mitigation
- Existing practices undertaken by each stakeholder in fraud deterrence and/or detection
- The value of hotlines and reporting programs for different stakeholder groups, including auditors, the board, and regulators
- Practical insights into effectively assessing and auditing hotlines and reporting programs

Investor participants expressed a view that much has taken place in the last 20 years that has driven higher audit quality and less fraud in the US capital markets.

INVESTOR EXPECTATIONS

Investors contextualized the following findings from the CAQ's 2024 Institutional Investor Survey, conducted in partnership with KRC Research during their discussion:

- Ninety percent (90%) of investors agreed that risks related to noncompliance and fraud play a role in their assessment of a company
- Fifty-six percent (56%) of investors believe that fraud goes undetected in the US corporate reporting ecosystem (frequently at 40% and very frequently at 16%)
- Among investors who believe noncompliance and fraud are frequently undetected, most say that regulators (37%) and public company management (32%) are responsible for better detection, followed by external auditors (17%) and boards and audit committees (14%)
- The plurality of investors believe that the US corporate reporting system is effective but could use updating, 45% believe that the US corporate reporting system to prevent or identify fraud needs some updating, and only 20% believe that the US corporate reporting system is not keeping pace with the fraud environment

Investors' outlook on fraud at US public companies: Investor participants expressed a view that much has taken place in the last 20 years that has driven higher audit quality and less fraud in the US capital markets, including SOX and the requirement for investment funds to have a Chief Compliance Officer. However, some felt that fraud is more likely to occur now, compared to about 10 years ago given the challenging and uncertain market conditions in today's environment. Many companies have high valuations and stock compensation plans in place for employees at varying levels, which provide incentives to maintain a high stock price that can result in financial gain.

Investor expectations: The investor participants shared their view that the investor community does not always have a deep understanding of the accounting and financial reporting requirements for complex matters at companies as they are not operating from inside the companies. Many investors expect auditors to have the best information to make judgments about such matters because they believe they have a view from inside the company. However, investor expectations vary depending on the type of investor:

- On one end of the spectrum, **short sellers** may be actively looking for fraud to benefit on the belief that there is a fraud before it is known.
- At the other end of the spectrum, **quantitative investors** typically hold a stock or a bond for a few minutes to a couple of days and are looking for a quick mispricing, rather than fraud.
- **Stock pickers, investors, and bondholders** typically hold an investment for months to years. Those investors do have concerns about fraud, but **they generally presume that the auditors have done what investors believe is their job.**

Defining the fraud to identify the problem: In addition to considering the differing perspectives of different types of investors, it's also important for all stakeholders to do a better job of refining the definitions of the different types of fraud. This will help to ensure that potential solutions and areas of enhancement, and the stakeholder group(s) who can affect them, are appropriately aligned to the problems identified (i.e., material financial statement fraud as opposed to technology-related frauds such as phishing, spam, cyberattack, etc.).

What could be improved to keep pace with the current environment: Investors look at a broad range of information to determine whether a business is sound and often believe that more stringency applied to internal controls and non-GAAP measures (e.g., KPIs) can foster a stronger anti-fraud environment. Some investors may still carry impressions from a pre-SOX environment and/or allow headlines about large corporate frauds to influence their assumptions about fraud occurrences at US public companies. The following represent actions (of which some may be existing requirements) that auditors and other members of the financial reporting ecosystem could take (if they are not already) that may be helpful to investors in informing their perspectives:

- Increase communication between investors and auditors about fraud
- Consider who auditors conduct inquiries with during the audit (in addition to financial and accounting personnel at companies)
- Engage in deeper discussions about CAMs
- Consider non-GAAP measures and KPIs
- Consider how ongoing internal control weaknesses inform risk assessment
- Consider third party risks and related party transactions
- Consider how the company's accounting policies compare to peers and how that informs risk assessment
- Maintain tight segregation of duties within companies

BIG IDEA

Due to expectations of stakeholders, investors view that the auditor's role could evolve by auditing and placing more emphasis on certain areas that may increase transparency with investors, such as non-GAAP measures and CAMs.

REMINDER

When discussing fraud, it is key to establish the *type* of fraud that is being referred to in order to implement appropriate controls and other measures to address it. The term "fraud" alone is too general.

EXISTING STAKEHOLDER ROLES, RESPONSIBILITIES AND PRACTICES

Participants explored each of the existing stakeholder roles and responsibilities and discussed leading practices. Participants discussed that internal controls alone are often not enough to deter and detect fraud and, therefore, companies need to implement multiple layers of defense by clearly defining roles and responsibilities. The mitigation of fraud risk is most effective when all participants of the financial reporting ecosystem fulfill their roles in deterring and detecting fraud.

Management and those charged with governance design and implement programs and controls to prevent, deter, and detect fraud.

Public company management and preparers: Management has a fiduciary obligation to investors and the public. Preparers have a responsibility to maintain accurate financial statements. A critical element to deter and detect fraud is the ethical tone at the top, as corporate culture can create an environment where management is empowered to prevent fraud. Transparency from those at the top of an organization also plays an important role, as it can encourage people to speak up and take corrective action sooner. Skepticism and intellectual curiosity should also be valued and encouraged within a company, as someone asking "the question beyond the original question" is often how fraudulent activity is uncovered.

Internal auditors provide assurance and insight into the adequacy and effectiveness of governance and the management of risk (including internal control).

Internal audit: The internal audit function is to strengthen governance, risk management, and control processes. Its impact extends beyond the organization as internal auditing contributes to an organization's overall stability and sustainability by providing assurance on its operational efficiency, reliability of reporting compliance with rules and regulations, safeguarding assets, and promoting an ethical culture. Global Internal Audit standards require that the internal audit plan considers fraud risk and the effectiveness of the organization's compliance and ethics programs (among other things).

Boards of directors and audit committees provide oversight of the financial reporting process and set the proper tone; create and maintain a culture of honesty and high ethical standards; and establish appropriate controls to prevent, deter, and detect fraud.

Boards and audit committees: A company's governance and oversight function have a responsibility to hold management accountable and should have a clear and defined process for doing so. For example, audit committees should have detailed discussions about fraud with management and take advantage of private sessions. In exploring the low percentage of fraud detected by external auditors, audit committee participants expressed that this was not alarming or unexpected as it signals that the other lines of defense and control systems are working. Participants discussed that the most common method for fraud detection is tips, followed by internal audit and management review.

BIG IDEA

Boards and management should promote a strong ethical culture throughout the company, with two-way dialogue at the forefront, by setting aside time to invest in an ethics and/or integrity day. Management should foster an environment where an ethical tone and values trickle down from the top to the middle and the bottom/beginning.

BIG IDEA

Private sessions and continuous dialogue with audit committees are key. When dealing with sensitive fraud-related matters, auditors should be intentional with the frequency and quality of information shared with the audit committee to best inform next steps.

BIG IDEA

It is critical for the board and audit committees to enforce consequences in response to fraud or other misconduct, in order to set a strong tone at the top. When management, or others, are held accountable, it further cements the values of the organization and reinforces an ethical culture.

External auditors plan and perform the audit to obtain reasonable assurance about whether the financial statements are free of material misstatement, whether caused by error or by fraud.

External audit: External auditors are expected to understand the company under audit and its processes and identify risks of such significance to require an audit response. Part of identifying risks includes understanding where incentives might be for people in the company to commit fraud. In order to do this, auditors ask key questions during walkthroughs that help to identify potential fraud risks, perform specific inquiries about fraud with appropriate people at the company, and identify and understand significant related parties and unusual transactions.

The three lines model underscores the importance of each line of defense working in concert to achieve strong governance and effective risk mitigation.

Cross-functional collaboration: With respect to US public companies, the lines of defense, and aforementioned stakeholder groups must work in concert to be as effective as possible in addressing and mitigating fraud risk. Although each stakeholder has a different role related to preventing, detecting, and addressing fraud, it is important that they collaborate with each other and avoid working in silos.

EFFECTIVE HOTLINE AND REPORTING PROGRAMS

Tips are the most common method to detect fraud at US public companies and other organizations. At US public companies, internal audit and management are also detecting fraud, often through data analytics, monitoring, and other robust systems of internal controls. Subject matter experts explored the following areas reported in NAVEX's 2024 Whistleblowing & Incident Management Benchmark Report:

- Report volume (1.57 reporters per 100 employees) and substantiation rates (45%) of reports received reached the highest levels ever—and both are good news.
  - Research has shown that higher rates of internal reporting translate to better business outcomes.
  - Programs that are successful in encouraging reporters to speak up have direct visibility into how these pressures are impacting their organizations, offering the opportunity to detect and mitigate risk.

- Accounting, auditing and financial reporting related reports, while lower in overage percentage of reports received internally at a median of 4.3%, often received an outsized share of attention. Additionally, accounting-related reports:
  - Had among the highest median substantiation rate at 50%.
  - Experienced the longest time to investigate and close the case.
  - Showed the longest time between when an incident was observed and when it was reported to the organization.
  - Accounted for twice as many of the reports submitted by third parties than the reports submitted by employees.

BIG IDEA

In considering the future of fraud detection and how the auditor's role could be strengthened, technology will likely provide meaningful opportunities. Auditors can perform more robust fraud risk assessments, develop thoughtful audit responses, incorporate unpredictability, and modify testing procedures (e.g., better identify outliers or unexpected items in a population) with access to more advanced technology and that continues to evolve over time.

- Third parties are more likely to report business integrity and financial misconduct issues.
  - Business integrity issues include conflicts of interest, vendor issues, fraud, global trade, and human rights.
  - These types of risks can impact several components of an organization's supply chain.

- Increase in report volume shows large payoff in healthy report mix.
  - Receiving a diverse mix of topics, inquiries, and allegations in an internal reporting system is a sign of programmatic health.
  - Organizations that make an effort to encourage internal reporting achieve significant improvements in the balance of risk categories received in their systems.

Hotline and reporting trends: Given that there remains a stigma with attaching the label "whistleblower" to someone who is doing what companies have trained them to do—reporting known or suspected wrongdoing—many US public companies refer to whistleblower hotlines as simply "hotlines" or "reporting" instead. A higher volume of hotline reports does not necessarily indicate more issues or a higher risk of fraud. It is a signal that the hotline is working and that there is trust in the company (i.e., employees trust management will do something), which is what companies should want from their programs.

Effective hotline and reporting programs: As hotline programs mature, employees become more familiar and comfortable with how to report and follow up. Ensuring that the hotline reports are anonymous and having a follow-up action in place are some of the top considerations for a successful hotline program. It is very important for companies to track that all reports have been addressed, including non-compliance matters that may appear unrelated to fraud.

Assessing and responding to hotline reports: When receiving and evaluating hotline reports, it is important to pay attention to more than just the compliance, accounting, and bribery and corruption issues, and not to ignore other types of reports that may be perceived as less important. Human resources matters and other "noise" are often indications of a company's culture and can point to far more serious issues, including financial related matters. By looking at hotline data holistically, companies may be able to identify direct or indirect correlations among different types of issues that could be important.

Use of hotline reporting data: A company's hotline is an important tool that can be used as part of fraud risk assessments, as the data collected from hotlines can be valuable in informing such risk assessments and the related audit plans/responses. For example, the volume and types of matters identified from the hotline reports can be considered in identifying specific types of risks that may be present at the company and/or in selecting the specific sites that will be visited or audited.

Third party reporting channels: For accounting related reports, twice as many of the reports were submitted by third parties as by employees. In FY2024, the SEC Office of the Whistleblower noted that 38% of whistleblowers who received rewards were individuals from outside of the organization. Therefore, there could be a missed opportunity to identify issues sooner for organizations that do not encourage third parties to report potential wrongdoings through their reporting system.

BIG IDEA

A framework around which management can be evaluated on how the hotline works and how effectively it works, and for auditors to understand the design and implementation of the hotline, would be beneficial to all members of the financial reporting ecosystem to assess hotlines effectively.

BIG IDEA

Current auditing procedures for hotlines can be potentially enhanced by further analyzing the data that is collected from the hotlines and understanding the underlying trends (e.g., cost centers, subsidiaries, supervisors, report types) and using the data to assess risk accordingly.

BIG IDEA

While a hotline can be a very important layer of control, research has shown that employees are often more likely to go to their supervisors to raise issues than to call a hotline. Companies should enable and encourage managers to respond to issues that may be reported to them and arm them with the tools to address such matters appropriately as a proactive mechanism to deter and detect fraud sooner.

Continuing to Strengthen Fraud Deterrence and Detection

Participants shared reactions in response to sessions on the current fraud risk landscape, emerging fraud risks, investor expectations, existing stakeholder roles and responsibilities, and effective hotline and reporting programs. The roundtable discussion facilitated a multi-stakeholder dialogue on how to continue to strengthen fraud deterrence and detection across the financial reporting ecosystem.

There was a general consensus that standards and principles can only go so far in the fight against fraud due to the "human element" of both the perpetration and detection of fraud.

THE FUTURE OF FRAUD DETERRENCE AND DETECTION

There was a general consensus that fraud is an inherent risk when considering the external pressures in the US capital markets, however, there were differing views on the likelihood and how to think about magnitude based on the nature of the fraud. Many were in agreement that the volume of material financial reporting fraud is small. This underscored the key takeaway that it is important to define the type of fraud when stakeholders are discussing the issue. There was also a general consensus that fraud cannot be eliminated completely. Deterring and detecting fraud comes at a cost with a point of diminishing returns. The question that remains, but can be difficult to answer, is what amount of fraud in the US capital markets can be tolerated from a cost/benefit perspective.

The financial reporting landscape is becoming more complex and the ways through which fraud is committed in the future could be very different from what they are today. Therefore, it is important for management and internal auditors as well as external auditors to identify the fraud risks and add fresh perspectives every year during fraud-related audit procedures (i.e., fraud brainstorming, fraud inquiries, unpredictable procedures, assessing hotlines). There was a general consensus that standards and principles can only go so far in the fight against fraud due to the "human element" of both the perpetration and detection of fraud. It is critical for all relevant stakeholders to stay vigilant as they fulfill their roles and responsibilities in this area. Below are practical insights into areas that can continue to be strengthened in effort to more effectively deter and detect fraud:

Fraud risk assessment: Fraud is generally considered a low likelihood event, but it can have a very significant impact. It was suggested that too much emphasis may be placed on the likelihood of fraud, rather than the impact of fraud, potentially preventing fraud from being detected more frequently. As the fraud risk landscape changes and evolves, so should the work of all gatekeepers (e.g., management, internal and external auditors).

Fraud brainstorming: Although it is not required by the auditing standards, involving forensic professionals in the fraud brainstorming sessions on a very routine basis can better inform the fraud risk assessment and other fraud-related audit procedures. Given that fraud brainstorming is performed at the beginning of the planning phase and knowing that the risk assessment is ongoing during the course of the audit, it is critical to elevate the sense of "if you see something, say something" when auditors leave the fraud brainstorming session.

Fraud inquiries: While quantitative procedures are important, qualitative procedures such as speaking directly to individuals whether as part of or apart from fraud inquiries are equally as important. Face-to-face interactions are a critical element of fraud-related auditing procedures, and asking very simple questions such as "Has anyone every asked you to do anything outside of this process?" can reveal transactions that could be vehicles for or indicators of fraud. Further, the manner in which process owners respond to questions can reflect their integrity and trust in the company, which can be signals to auditors as well.

Use of technology: Investing in technology is potentially one of the most impactful areas where the detection of fraud can be strengthened. Advances in technology can provide opportunities for management and internal auditors as well as external auditors to work more efficiently and free up more time to focus on complex matters. However, companies and their auditors should be aware of the risks and biases that come with implementing and using new technologies, such as artificial intelligence, and make sure that they address those risks because these are very powerful tools that can be used to harness large amounts of data.

Access to data: Participants further discussed the importance of access to company data. The general consensus was that, while internal and external auditors' access to company data is not limited, at times there are challenges in using that data (e.g., capacity of company systems, identifying reasonable and effective ways to use enormous datasets, considerations related to sufficient, appropriate audit evidence, shift in skillsets needed by auditors/audit teams).

Assessing hotlines: Hotlines and reporting programs are an area to which financial reporting stakeholders can pay more attention for purposes of informing their fraud-related procedures. This is also potentially an area to explore whether updated guidance for management could be developed and/or whether specific requirements could be built into auditing standards in order to promote consistency in the procedures auditors perform related to hotlines. In addition to assessing a hotline for its effectiveness, using the data that is collected from the hotline is also important as it can reveal a trove of valuable information, such as the company's culture and trust in using the hotlines, in addition to potential indicators of fraud.

Culture and ethics: Just as the "human element" is an important factor in how and why frauds are committed, it is also relevant in the prevention and detection of fraud. A company can have an extremely robust compliance program on paper, but if the company's culture and values do not embrace compliance, then its programs will likely not be effective. Having a strong ethical culture and ethically minded employees is a critical factor in fraud deterrence and detection. And companies need to enforce their culture by asking what actions will be taken and what the consequences will be for those who do not embody a culture of integrity and compliance.

Training: Training for management and internal auditors as well as external auditors is one of the most important areas to continually enhance the awareness of fraud and provide staff of all levels with tools to identify and report risks of fraud. More training can be provided on how fraud is committed and the mindset of looking for fraud. Junior

Having a strong ethical culture and ethically minded employees is a critical factor in fraud deterrence and detection.

staff should also feel empowered during fraud discussions and be encouraged to probe and ask questions, as they are often closest to the details. As the fraud risk landscape continues to evolve, the attitudes and professional skepticism of the members of the financial reporting ecosystem will need to be applied to an evolving landscape, in order to continue to recognize and respond to current and emerging fraud risks.

CONCLUSION

Remaining vigilant, including exercising professional skepticism and having a questioning mind, remains vitally important for every member within the financial reporting ecosystem in the fight against fraud. As financial reporting fraud continues to be at the forefront of the public interest, finding the balance between standards, regulations, and investor protection is important to the durability and attractiveness of the US public markets.

Auditing standards will require feedback from a diverse group of stakeholders. Therefore, it is critically important to engage in an ongoing open dialogue about fraud-related procedures and the responsibilities of the auditors and other stakeholders—what they are and what they are not—in order to instill public trust in the capital markets and high-quality audits. As a result of this inaugural Fraud Forum, the CAQ and AFC seek to continue the dialogue and engage with stakeholders, investors, and regulators to advance the discussion of critical anti-fraud efforts.

Remaining vigilant remains vitally important for every member within the financial reporting ecosystem in the fight against fraud.

Appendix:

AFC Fraud Forum Participants and Observers

Name	Company	Title
Tony Anderson	Independent Director	Audit Committee Chair
Jill Austin	IIA	Senior Manager, Professional Issues
Julie Bell Lindsay	CAQ	Chief Executive Officer
Thedore Bunting	Independent Director	Audit Committee Chair
Tim Carey	PwC	National Office Leader
Jill Chiarello	Accenture	Internal Controls, Director
Jack Ciesielski	R.G. Associates	President
Cynthia Cooper	The CooperGroup	Chief Executive Officer
Erin Cromwell	CAQ	Manager, Professional Practice
Brian Croteau	PwC	US Chief Auditor
Liz Crowe	FEI	Professional Accounting Fellow
Brian Degano	PCAOB	Associate Chief Auditor, Office of Chief Auditor
Linda Delahanty	AICPA	Technical Director, Audit & Attest Standards
Anita Doutt	SEC	Senior Associate Chief Accountant
Megha DSa	SEC	Professional Accounting Fellow
Candace Duncan	Independent Director	Board Member
Jessica Echenique	IIA	International Internal Audit Standards Board
Julie Edwards	PCAOB	Board Advisor
Chris Ekimoff	RSM	Director, Financial Investigations & Dispute Services
Julia Germain	CAQ	Senior Manager, Communications
Jonathan Gregory	The Hershey Company	Corporate Controller
Donnie Heinerichs	CAQ	Manager, Professional Practice
Christina Ho	PCAOB	Board Member
Soyoung Ho	Thomson Reuters	Senior Editor
Wes Kelly	Crowe	Partner

Name	Company	Title
Katrina Kimpel	EY	Americas Vice Chair
Jennifer Knecht	Crowe	Partner
Raphael Larson	King & Spalding	Partner
Sara Lord	RSM	Chief Auditor
Emily Lucas	CAQ	Fellow, Professional Practice
Rachel Marra	PwC	National Office Managing Director
Dennis McGowan	CAQ	Vice President, Professional Practice
Andi McNeal	ACFE	Chief Training Officer
Mandy Moody	ACFE	Vice President, Communications
Steve Morrison	CohnReznick	Partner, National Director of Audit
Naohiro Mouri	AIG	Executive Vice President and Chief Auditor
Dan Murdock	Comcast Corporation	Executive Vice President and Chief Accounting Officer
Jason Nagler	Investment Company Institute	Senior Director, Fund Accounting & Compliance
Mayur Patel	FINRA	Senior Principal Intelligence Specialist
Sonali Patel	Mayer Brown	Partner
Robert Peak	PCAOB	Board Advisor
Carrie Penman	NAVEX Global	Chief Risk and Compliance Officer
Christian Peo	KPMG	National Managing Partner
Bill Pollard	Deloitte	Partner
Steven Richards	Ankura Consulting	Senior Managing Director
Kelly Richmond Pope	DePaul University	Dr. Barry Jay Epstein Endowed Professor of Forensic Accounting
Amy Rojik	BDO	Assurance Managing Principal
Matthew Schell	Crowe	Managing Partner
Annette Schumacher	CAQ	Senior Director, Professional Practice
Matt Sickmiller	PCAOB	Assistant Chief Auditor
Elizabeth Sullivan	WMATA	Vice President, Chief Risk and Audit Officer
John Treiber	Deloitte	Chief Risk Officer
Lucy Wang	CAQ	Director, Anti-Fraud Initiatives

AFC

www.antifraudcollaboration.org

We welcome your feedback!

Questions or comments?
Visit antifraudcollaboration.org/contact