tapestry NETWORKS

ACN VIEWPOINTS

Combating corporate fraud: how audit committees oversee fraud risk

August 2024

Fraud risk remains a persistent concern for audit committees despite decades of advances in fraud prevention and detection. Some audit chairs worry that fraud does not receive sufficient attention amid increasingly crowded audit committee agendas; others wonder if discussions have kept pace with evolving fraud risks in a world rife with novel technology vectors.

From February to June 2024, Tapestry Networks convened six in-person meetings of its regional US audit committee networks, bringing together audit committee chairs of large US public companies to discuss the challenges of modern fraud risk oversight. Amanda Massucci, EY Pacific Southwest Forensics Leader, also contributed insights at our meetings.

For a list of reflection questions for audit committees, see page 10. For the list of participating audit chairs, see Appendix 1 (page 12), and for the guest's biography, see Appendix 2 (page 16).

This *ViewPoints*[1] covers key themes that emerged from the meetings and related conversations:

EY Building a better working world

Traditional and modern fraud schemes are part of an evolving risk landscape

Fraud remains a dynamic and persistent issue for companies, evolving as quickly as new fraud vectors are discovered. According to the Association of Certified Fraud Examiners (ACFE), organizations lose 5% of their revenue to fraud each year.[2] Despite the success of the Sarbanes-Oxley Act (SOX) in reducing major collusive financial frauds in the US, fraud in all its forms persists. As EY's Ms. Massucci said, *"Fraud is alive and well"* and includes basic frauds as well as more sophisticated schemes.

What is fraud?

Fraud is a broad term with varying definitions. For the purposes of this document, fraud is any activity that relies on deception in pursuit of illicit gain. Whether any given incident of fraud constitutes a criminal act depends on jurisdiction-specific legal elements beyond the scope of our discussions. Rather than addressing the legal consequences of fraud, this document focuses on matters of governance aimed at the prevention and detection of fraud.

The covert nature of fraud presents a challenge to assessing its prevalence and sorting it by type. ACFE's *Occupational Fraud 2024: A Report to the Nations*, which analyzed over 1,900 real-world fraud cases from 138 different countries and territories and 22 industry categories, provides some insights. The report reveals that 89% of reported frauds involved asset misappropriation, and 5% represented higher-value financial statement frauds.[3] EY's *Global Integrity Report 2024* offers additional insights, highlighting a rise in corporate misconduct: nearly one in five organizations experienced a significant integrity incident—such as a major fraud, data privacy and security breach, or regulatory compliance violation—in the past two years, often involving third parties.[4]

During discussions, members emphasized that the fraud triangle—pressure, opportunity, and rationalization—remains a useful framework for identifying and assessing fraud risk. They highlighted several factors in today's business environment that may tend to increase the risk:

- **Economic volatility.** *"The economy impacts all three sides of the fraud triangle,"* Ms. Massucci said. Pressure and incentive go up in times of economic hardship, and companies may unintentionally weaken their control environment by tightening budgets.
- **Remote and hybrid working.** *"How do you build and maintain a consistent culture without having people meet at the water cooler or face-to-face with top executives?"* one audit chair worried. Another said loyalty is a concern: *"People are not as loyal to companies since they started working from home. They also don't report issues, which creates risk. There's rampant dishonesty and a high tolerance for it."*

- **Talent challenges.** Workforce reductions, employee turnover, and other personnel changes may compromise control environments and culture. The well-documented finance talent shortage exacerbates these challenges.[5]
- **Shifting generational attitudes.** Some members worried that younger generations lack appropriate training. *"Young employees seem to be less skeptical and don't show enough critical thinking skills,"* one said.
- **New technologies.** Technology has significantly affected how frauds are perpetrated. *"The scary thing is how fraud schemes are ever changing, and technology is making them more sophisticated and believable,"* a member said.
- **Regulatory landscape.** Increasingly complex reporting standards and regulations create new pathways for fraud. The changing regulatory environment requires continuous monitoring; companies need to constantly adapt to mitigate risks.
- **Reputational risks.** In today's interconnected world, even minor frauds can quickly escalate into significant reputational issues.

Members discussed various types of fraud assailing their companies, highlighting the following:

- **Traditional financial frauds (e.g., financial statement fraud, asset misappropriation, kickbacks).** *"More sophisticated frauds are happening, but the basics are still there, like asset misappropriation, bribery, corruption*," said Ms. Massucci. One member observed, *"I haven't seen as much of the major, collusive sorts of fraud post-SOX, but I have seen things like bribery and noncompliance with the Foreign Corrupt Practices Act [FCPA]."* Ms. Massucci noted that acquisitions and new ventures can pose heightened financial fraud risks: *"So many companies have expanded through acquisitions, starting new businesses, entering new geographies. We've seen challenges when clients get into something new, which is exciting, but compliance risks may not be looked at as closely as they should be. Performing effective due diligence helps mitigate the risk."*
- **Intellectual property fraud.** *"Employees stealing intellectual property by whatever means available is a concern. Typically it happens outside the US by people who want US technology,"* one member said, advising companies to *"make sure only the necessary people have access, and no more."*
- **Environmental, social, and governance (ESG) fraud.** Most audit chairs reported that their companies are still in the early stage of ESG reporting. Some companies have begun to establish systems and controls for ESG reporting, with some limited discussion of potential fraud risks from the disclosure of ESG information. *"We're so worried about getting to the climate data itself that we're not worried yet about the potential for fraud,"* one said. But all audit chairs acknowledged the increased fraud risk related to nonfinancial reporting. *"If compensation has elements tied to climate*

targets, then you need to consider an elevated fraud risk," a member observed. Another said, *"I think we probably need to dive deeper into the controls related to ESG and climate reporting, to step back and identify where the fraud risks are and identify areas that we need to tighten up."*

- **External frauds (e.g., third-party fraud, cyber fraud).** External frauds are committed by individuals outside an organization, such as customers, vendors, and cybercriminals. One member noted that her company is *"spending a lot more time"* on third-party risks. Members also emphasized how *"inextricably linked"* cyber risk and fraud are. While not all cyberattacks constitute fraud, those involving deception for financial or personal gain, such as phishing schemes or deepfakes, do.

Lessons from real-world frauds

Falsified sales records

One audit chair described a fraud involving a sales team falsifying sales records, where the fraudsters were motivated by bonus incentives. It occurred at an *"insignificant subsidiary that became significant,"* the audit chair said. The corporate finance team discovered the fraud and reported it. An investigation led to the firing of most of the subsidiary's staff. The subsidiary was eventually shut down and its assets sold. *"We thought we had the right controls and that we were buttoned up from an accounting perspective,"* said the audit chair, but after the fraud, the parent company realized several red flags had not been considered, such as the rapid increase in sales, frequent changes in finance staff, and the dispersed workforce.

Insider threat and reputational damage

"We discovered a cyber fraud that exposed our lack of focus on insider threats," an audit chair said. In this case, a cybercriminal induced one of the company's employees in a foreign country to sell their credentials, allowing access to the company's systems. The cybercriminal used this access to obtain information about the company's top clients, subsequently publishing the details on the dark web. Though the breach was discovered and shut down *"within the hour"* and there was no immediate financial damage, *"it caused significant embarrassment and reputational damage."* The audit chair cautioned others to ensure their companies adequately consider insider threats, especially in foreign operations.

Suspicious activity after a key announcement

One company experienced a fraud immediately following the announcement of a significant transaction. Fraudsters used AI-generated "internal" phone calls to request transfers of money. *"They had account numbers and all the information they needed. If there had not been a conversation about the transfers in a secure environment, the money would probably have been sent because it was timed so perfectly with the transaction,"* the audit chair said. A lengthy investigation concluded that there were internal and external parties involved in the fraud, which could have resulted in an erroneous wire transfer of $100 million.

The rising incidence of cyber fraud has prompted enhanced security and training

Audit chairs discussed their companies' responses to increasingly sophisticated cyber frauds, particularly those driven by AI, such as cloned voices and deepfake videos. For example, Deborah Wheeler, Delta Air Lines' chief information security officer, reported that Delta experienced *"a 900% increase in the number of phishing events coming out of the pandemic versus the years leading into it"* and noted that AI-generated phishing emails are now highly convincing and lack typical telltale signs (i.e., typos, poor grammar, etc.) of a fake email.[6] Identity theft and other advanced intrusion techniques have also become more common.

Members discussed a recent incident where an employee at a UK architecture and design firm transferred the equivalent of $25.6 million to fraudsters after being deceived by deepfake videos of the CFO and other staff.[7] This sort of fraud underscores the need for enhanced security measures and training and aligns with major themes discussed during the meetings:

- **Verify, verify, verify.** There's a growing recognition that electronic controls are not fully reliable. *"There is a need to go back to the basics,"* one audit chair said. Members described a range of measures implemented at their companies, such as *"hanging up and calling back,"* if, for example, the CEO requests something. This was a point Ms. Wheeler also emphasized in a recent discussion with the Audit Committee Leadership Network. She stressed the need for "out-of-band verification"—a method to validate information through a separate, independent channel. *"Pick up the phone and contact the individual on a known number or stop by their office. Have an external way of validating the authenticity of what you're being sent. Use a code word,"* she advised.[8]

READ MORE »

Audit Committee Leadership Network ***ViewPoints: Cybersecurity and Data Privacy: A Dialogue with Chief Information Security Officers and Data Privacy Leaders***

- **Strengthen awareness and training at all organizational levels.** Employees are one of the biggest areas of vulnerability for a company: one click on a phishing email can compromise the security of the entire company. *"Employees need way more training today because you can't trust anything,"* a member said. Several audit chairs reported that their companies have increased training not only for employees, but also for boards. One company's CFO created an avatar of herself which she shared with staff and board members to demonstrate how unreliable visual representations can be; she advised her staff to trust only in-person communications with her. Another member shared a similar experience: *"Management took video clips of our CEO doing earnings presentations and created a few vignettes of a fake version of the CEO giving fabricated talks. They showed it to the board to open our eyes to*

what could be done. It got our attention."

- **Employ advanced technologies to combat cyber fraud.** Companies should explore how to use advanced technologies like AI for defense. These tools can help evaluate risk factors, analyze trends, and quickly reprioritize efforts as necessary. A recent Tapestry Networks' survey of fraud risk management professionals at large global companies underscored the point. One survey respondent noted that *"leveraging data and emerging technologies will be critical to keep up with the pace of the ever-changing risk landscape."*

Leading audit committees are taking a proactive oversight approach

Effective fraud risk oversight is a crucial yet challenging responsibility for audit committees, and it requires a comprehensive, proactive approach. Key themes and good practices that emerged in the discussions included the following:

- **Fraud affects many different functions: internal collaboration is essential.** To manage fraud risk effectively, companies should avoid operating in silos. *"First of all, management must acknowledge that fraud is a real risk. Then there are all the supporting systems: legal, internal audit, IT, security, culture, whistleblower frameworks, etc.,"* an audit chair said. Many audit chairs reported using the "three lines of defense" model, with management, risk management and compliance, and internal audit each playing a distinct and vital role in fraud prevention and detection. Audit committees must ensure that appropriate frameworks, processes, and controls are in place; members noted that internal audit is a key partner in this work. They highlighted other good practices as well:
    - **Encourage information sharing across the organization.** Audit committees must consider information from the many functions involved in fraud prevention and detection efforts. Ms. Massucci advised audit chairs to ask, *"How is all of the information being consolidated to provide the full picture?"* This point was underscored by the audit chair of a large global European company in Tapestry's publication *Combating Corporate Reporting Fraud*: *"The more we can compile data from various company sources, the more chance we have of picking up potential issues."*[9] That company created a common database for internal audit issues, compliance reports, finance data, culture surveys, whistleblower complaints, and other relevant information like health inspections to analyze the integrated data for outliers and trends.
    - **Be prepared.** Establishing processes and controls is only part of the battle: using them is equally important. A member noted, *"The general counsel must be well*

trained on when to engage or escalate issues to the audit committee. Otherwise, they may discover an issue, do their own investigation, and by the time they inform the audit committee or board, it is further down the line, and that doesn't create a good record of governance." Another member recommended incorporating communication plans and escalation processes into tabletop exercises and ensuring management and board members are involved in these practices.

- **Leverage the chief compliance officer.** Ms. Massucci encouraged audit chairs to have regular, substantive discussions with the chief compliance officer. *"There is a treasure trove of information there,"* she said. However, the level of interaction between compliance officers and the audit committee varies widely by company—some have monthly meetings, and some get only a few minutes each year. *"Some chief compliance officers say it could be beneficial for the organization if they had more time with the board to discuss compliance risks,"* Ms. Massucci said.

COMPANIES EXPLORE WAYS TO ENHANCE INFORMATION SHARING

In Tapestry Networks' recent global survey of fraud risk management professionals, one respondent highlighted a company's approach of assigning *"designated owners by fraud type"* to lead discussions on trends and improvement opportunities. The company also launched a *"fraud summit to enhance information sharing across teams involved in fraud prevention and detection activities."*

- **The role of culture cannot be overstated.** *"There's no substitute for a strong message of integrity and ethics and having them be core parts of the culture,"* a member stressed. Audit chairs noted that culture impacts both the likelihood of fraud and employees' willingness to report issues but acknowledged that it is difficult to assess culture accurately, especially in large companies. They highlighted key considerations:
  - **Ensure the CEO and board set an appropriate tone at the top.** *"Fraud is a symptom of a breakdown of the ethical culture of a company, and if one person is responsible, it's the CEO,"* a member said. Regular, clear communication tailored to all the company's various audiences is needed to reinforce ethical standards. The board also contributes to setting the tone. Another member noted that boards should be *"mindful of how we react when things happen"* so as to encourage transparency and ensure management remains willing to speak up.
  - **Assess the "mood in the middle."** Audit chairs emphasized the need to understand how senior leadership's tone is perceived and adopted by mid-level management and employees. *"Your leadership team may believe they are setting the right standard, but the reality can be different,"* one said. Another

noted that internal audit can help audit chairs assess that mood. And another suggested adding specific questions to culture surveys to gain deeper insights.

- **Conduct site visits.** In addition to other forms of culture assessment, in-person site visits can help boards gain a more accurate picture of a company's culture. *"Do site visits and get back to the basics to get a better sense of the tone of the management teams on the ground. It is governance by walking the halls,"* one member said.
- **Don't overlook contractors.** An audit chair cautioned that *"contractors need to be trained to your company's rules and standards."* Audit committees should ensure that contractors' compliance and integrity frameworks are considered as part of fraud risk assessments, *"especially in international business, where there is always judgment around FCPA and anti-bribery rules."*

READ MORE »

Ethics, Compliance, and Culture Network: *Assessing Corporate Culture: A Practical Guide to Improving Board Oversight*

- **Whistleblower systems are an important tool to combat fraud.** ACFE's 2024 global study on fraud found that 43% of fraud cases were uncovered by whistleblower tips—more than three times the rate of internal audit, the next most common fraud detection method.[10] Organizations with hotlines were more likely to discover fraud than those without.[11] Audit chairs discussed different approaches to overseeing hotlines. For example, some review all parts of the hotline reports, while others review a summary of trends and key issues. Ensuring employee awareness and trust in the system is essential. This extends to vendors and customers as well: the ACFE report revealed that while 52% of tips come from employees, nearly one-third come from vendors and customers.[12]
- **Audit committees can explore opportunities to sharpen fraud risk oversight.** Members discussed key focus areas to help audit committees strengthen oversight:
  - **Proactively update fraud risk assessments.** Fraud risk is dynamic and requires continuous monitoring. Fraud risk assessments should be regularly updated and new types of fraud risk taken into consideration. To help identify evolving threats, one member suggested asking management questions along the lines of *"Where are we more vulnerable to fraud this year compared to last year?"* Ms. Massucci advised audit chairs to ask if management has *"taken a fresh look"* at the fraud risk assessment to avoid *"something that just rolled off the shelf."*
  - **Collaborate with the external auditor.** Audit committees should cultivate a collaborative relationship with external auditors that goes beyond routine inquiries about known or suspected fraud. One member worried that the

sophistication of fraud conversations has not changed to keep pace with changes in the risk landscape. But with more regulatory focus on the horizon—both the International Auditing and Assurance Standards Board and the US Public Company Accounting Oversight Board have upcoming projects on fraud[13]—members acknowledged that it is increasingly important to move past a *"check-the-box"* approach.

- **Ask targeted questions about fraud-related training.** Employee training is essential: fraud awareness training can "reduce fraud losses and ensure frauds are caught more quickly."[14] Trained employees are also twice as likely to provide hotline tips as employees who are not regularly trained in fraud risks.[15] Audit committees may find it valuable to ask management targeted questions about training. *"When I was a CFO, we dedicated a half-day of training for anyone handling company funds,"* one member observed. *"As an audit chair, I'm realizing maybe I should inquire about this type of training in my current company."* Another suggested asking management, *"Is there a risk-based analysis to determine who needs fraud-related training and what type of training they require?"*

HOW CAN AUDIT COMMITTEES STAY INFORMED ON FRAUD TRENDS?

Staying updated on significant and new fraud schemes can help audit committees ensure their companies have robust processes in place to mitigate risks. But one member asked, *"Is anyone tracking the most current fraud cases? We could all find an example in a textbook, but is it current?"* Members stay informed by following news and sharing examples in discussions like those hosted by Tapestry Networks, but they acknowledged that keeping up-to-date is challenging. One reflected, *"It's a good idea. And we should also ask how audit partners keep up with the latest schemes."*

Reflection questions for audit committees

- ? What type of fraud risks are the highest priority for your company? How have these priorities changed in recent years? How does your company and audit committee monitor how fraud risks may change?
- ? How does your company address potential sustainability-related fraud risks? How might sustainability matters raise fraud risk for your company in the coming years?
- ? How does your company use technology or AI for fraud prevention, monitoring, and detection? How comfortable are you with your understanding of how these technologies are being deployed? What concerns do you have?
- ? How do you satisfy yourself that the company's attitude toward fraud is understood throughout the company and that management maintains an appropriate culture?
- ? How does your audit committee assess culture as part of fraud risk assessments? How effective do you find these assessments to be?
- ? How are employees made aware of the company's fraud risk governance policies, including the handling of fraud-related incidents?
- ? What type of fraud-related training do employees receive? Are the appropriate risks considered when determining who needs fraud-related training and what type of training should be provided?
- ? How confident are you that fraud risk is effectively owned, assessed, and communicated across internal functions (e.g., compliance, legal, risk)? What gaps need to be addressed?
- ? How does your company integrate data from different functions involved in fraud risk management when assessing fraud risks? What additional data or analysis could be useful to help prevent and detect fraud?
- ? How effectively does your company collect, respond to, report on, and escalate whistleblower tips? Are hotlines effectively promoted to employees, vendors, and customers?

About this document

The Regional Audit Committee Networks are a group of audit committee chairs drawn from leading North American companies committed to improving the performance of audit committees and enhancing trust in financial markets. The network is organized and led by Tapestry Networks with the support of EY as part of its continuing commitment to board effectiveness and good governance.

ViewPoints is produced by Tapestry Networks to stimulate timely, substantive board discussions about the choices confronting audit committee members, management, and their advisers as they endeavor to fulfill their respective responsibilities to the investing public. The ultimate value of *ViewPoints* lies in its power to help all constituencies develop their own informed points of view on these important issues. Those who receive *ViewPoints* are encouraged to share it with others in their own networks. The more board members, members of management, and advisers who become systematically engaged in this dialogue, the more value will be created for all.

The perspectives presented in this document are the sole responsibility of Tapestry Networks and do not necessarily reflect the views of network members or participants, their affiliated organizations, or EY. Please consult your counselors for specific advice. EY refers to the global organization and may refer to one or more of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. Tapestry Networks and EY are independently owned and controlled organizations. This material is prepared and copyrighted by Tapestry Networks with all rights reserved. It may be reproduced and redistributed, but only in its entirety, including all copyright and trademark legends. Tapestry Networks and the associated logos are trademarks of Tapestry Networks, Inc., and EY and the associated logos are trademarks of EYGM Ltd.

Appendix 1: Participants

West Audit Committee Network-South—February 26, 2024

The following members participated in all or part of the meeting:

Mark Foletta, Dexcom and Enanta Pharmaceuticals
Leslie Heisz, Edwards Lifesciences
Bala Iyer, Power Integrations
Leon Janks, PriceSmart
Pat Kinsella, PennyMac Financial
Tim Leyden, Itron
Jim Morris, Edison International
Dick Poladian, Occidental Petroleum
Dilek Samil, Algonquin Power & Utilities Corp
Daren Shaw, Ensign Group
Les Sussman, East West Bancorp
David Tehle, Jack in the Box, National Vision, and US Foods

EY was represented by the following:

Robyn Bew, Director and West Region Leader - Center for Board Matters
Paul Chen, Greater LA Audit Practice Leader
Jennifer Lee, Managing Director, Americas Center for Board Matters
Pat Niemann, Partner, Americas Center for Board Matters

Tapestry Networks was represented by the following:

Beverley Bahlmann, Executive Director
Kate Cady, Project and Event Manager Team Leader
Kelly Gillen, Senior Associate
Jason Watkins, Managing Director

Central Audit Committee Network—March 11, 2024

The following members participated in all or part of the meeting:

Stuart Burgdoerfer, Progressive
Pat Condon, Entergy
Cheryl Francis, Morningstar
Frank Jaehnert, Nordson
Ginger Jones, Tronox Holdings
Cary McMillan, Hyatt Hotels
Ingrid Stafford, Alumna
Darrell Thomas, Pitney Bowes

Phoebe Wood, Invesco and Leggett & Platt
Carol Yancey, BlueLinx

EY was represented by the following:

Pat Niemann, Partner, Americas Center for Board Matters
Dave Sewell, US-Central Assurance Managing Partner

Tapestry Networks was represented by the following:

Beverley Bahlmann, Executive Director
Kate Cady, Project and Event Manager Team Leader
Kelly Gillen, Senior Associate
Jason Watkins, Managing Director

Southwest Audit Committee Network—March 25, 2024

The following members participated in all or part of the meeting:

Lee Canaan, EQT
Vanessa Chang, Transocean
Ryan Edone, LGI Homes
Donna Epps, Texas Pacific Land Corporation and Texas Roadhouse
Tom Gilligan, KB Home
Gerry Laderman, Kemper
Holli Ladhani, Marathon Oil
Gil Marmol, Foot Locker
Angela Minas, Vallourec
Don Robillard, Cheniere and Helmerich & Payne

EY was represented by the following:

Robyn Bew, Director and West Region Leader - Center for Board Matters
Kaki Giauque, Assurance Partner
Scott Hefner, Senior Global Client Service Partner
Pat Niemann, Partner, Americas Center for Board Matters
Sandra Oliver, US-West Assurance Managing Partner

Tapestry Networks was represented by the following:

Beverley Bahlmann, Executive Director
Kate Cady, Project and Event Manager Team Leader
Todd Schwartz, Executive Director
Jason Watkins, Managing Director

East Audit Committee Network—May 30, 2024

The following members participated in all or part of the meeting:

Bert Alfonso, Eastman Chemical Company
C. E. Andrews, Marriott Vacations Worldwide
Mark Besca, Markel Group
Mary Choksi, Omnicom Group
Mary Ann Cloyd, Fresh Del Monte Produce
Marie Gallagher, Glatfelter
Art Garcia, ABM Industries and American Electric Power Company
Mary Guilfoile, Interpublic Group
Marcy Reed, Clean Harbors
Judy Schmeling, Constellation Brands
Gina Wilson, Charles River Laboratories

EY was represented by the following:

Jennifer Lee, Managing Director, Americas Center for Board Matters
Anthony Sgammato, Partner
Alysia Steinmann, Metro New York Office Managing Partner
Steve Wanner, US-East Region Vice Chair

Tapestry Networks was represented by the following:

Noni Abdur-Razzaq, Associate
Beverley Bahlmann, Executive Director
Ashley Vannoy, Project and Event Manager
Jason Watkins, Managing Director

West Audit Committee Network-North—June 11, 2024

The following members participated in all or part of the meeting:

Kimberly Alexy, Western Digital
Prat Bhatt, Seagate Technology
Teresa Briggs, DocuSign, ServiceNow, and Warby Parker
Earl Fry, Hawaiian Holdings
Laurie Hodrick, Roku
Bala Iyer, Power Integrations
Jack Lazar, GlobalFoundries and Resideo Technologies
Mary Pat McCarthy, Micron Technology and Palo Alto Networks
Lou Miramontes, Lithia Motors
Karen Rogge, Onto Innovation

Janet Woodruff, Altus Group

EY was represented by the following:

Robyn Bew, Director and West Region Leader - Center for Board Matters
Scott Hefner, Senior Global Client Service Partner
Jennifer Lee, Managing Director, Americas Center for Board Matters

Tapestry Networks was represented by the following:

Kate Cady, Project and Event Manager Team Leader
Jonathan Day, Chief Executive
Kelly Gillen, Senior Associate
Jason Watkins, Managing Director

Southeast Audit Committee Network—June 25, 2024

The following members participated in all or part of the meeting:

Art Beattie, PPL Corporation
Denise Dickins, Watsco
Teri Fontenot, AMN Healthcare Services (Southwest Audit Committee Network member)
Tom Hough, Equifax
Jim Hunt, Brown & Brown
Mercedes Johnson, Synopsys and Teradyne
Rich Macchia, Corpay
Maria Pinelli, International Game Technology
Mimi Thigpen, Globe Life
Darrell Thomas, British American Tobacco
Susan Ward, Saia
Carol Yancey, BlueLinx Holdings
Bryan Yokley, Rayonier Advanced Materials

EY was represented by the following:

Pat Niemann, Partner, Americas Center for Board Matters

Tapestry Networks was represented by the following:

Beverley Bahlmann, Executive Director
Kate Cady, Project and Event Manager Team Leader
Tiffany Luehrs, Associate
Jason Watkins, Managing Director

Appendix 2: Guest biography

Amanda Massucci is the EY Pacific Southwest Forensics Leader. She works with clients on complex compliance and financial matters. Ms. Massucci assists a diverse base of clients across industries, including highly regulated industries. She works with in-house investigative counsel, compliance teams, internal audit, and outside counsel.

Ms. Massucci has experience conducting large accounting and financial fraud investigations. The issues addressed in these investigations include revenue recognition, earnings management, inappropriate accounting for reserves, and disclosure requirements. Because of her investigative experience, she also assists EY clients in litigation matters, the assessment of internal controls, and the prevention and detection of fraud.

Ms. Massucci assists her clients in connection with global anti-bribery and corruption matters. She leads global investigations, performs due diligence on potential acquisition targets, and conducts bribery and corruption compliance assessments. She has also assisted clients in the design, implementation, and monitoring of compliance programs.

Endnotes

[1] *ViewPoints* reflects the network's use of a modified version of the Chatham House Rule whereby names of members and their company affiliations are a matter of public record, but comments are not attributed to individuals or corporations. Italicized quotations reflect comments made in connection with the meeting by network members and other meeting participants.

[2] Association of Certified Fraud Examiners, *Occupational Fraud 2024: A Report to the Nations* (Austin, TX: Association of Certified Fraud Examiners, Inc., 2024), 9.

[3] Association of Certified Fraud Examiners, *Occupational Fraud 2024: A Report to the Nations*, 7, 10.

[4] EY, *Global Integrity Report 2024*, (London, EYGM Limited, 2024), 7.

[5] Mark Maurer, "The Accountant Shortage Is Showing Up in Financial Statements," *Wall Street Journal*, July 11, 2023.

[6] Audit Committee Leadership Network, *Cybersecurity and Data Privacy: A Dialogue with Chief Information Security Officers and Data Privacy Leaders*, ViewPoints (Waltham, MA: Tapestry Networks, 2024), 2.

[7] Heather Chen and Kathleen Magramo, "Finance Worker Pays Out $25 Million after Video Call with Deepfake 'Chief Financial Officer,'" CNN, February 4, 2024.

[8] Audit Committee Leadership Network, *Cybersecurity and Data Privacy: A Dialogue with Chief Information Security Officers and Data Privacy Leaders*, 4.

[9] Tapestry Networks, *Combating Corporate Reporting Fraud: Learnings from Leading European Audit Committee Chairs* (Waltham, MA: Tapestry Networks, 2023), 10.

[10] Association of Certified Fraud Examiners, *Occupational Fraud 2024: A Report to the Nations*, 23–24.

[11] Association of Certified Fraud Examiners, *Occupational Fraud 2024: A Report to the Nations*, 23.

[12] Association of Certified Fraud Examiners, *Occupational Fraud 2024: A Report to the Nations*, 23–24.

[13] International Auditing and Assurance Standards Board, "IAASB Moves to Strengthen Auditors' Efforts Related to Fraud," news release, February 6, 2024; "Standard-Setting, Research, and Rulemaking Projects," Public Company Accounting Oversight Board, mid-term standard-setting project on fraud, accessed August 22, 2024.

[14] Association of Certified Fraud Examiners, *Occupational Fraud 2024: A Report to the Nations*, 42.

[15] Association of Certified Fraud Examiners, *Occupational Fraud 2024: A Report to the Nations*, 42.