tapestry NETWORKS

ACLN SUMMARY OF THEMES

SEC developments, Supreme Court implications, risk oversight, and cybersecurity

November 2023

On November 9-10, 2023, members of the Audit Committee Leadership Network (ACLN) met in Washington, DC to discuss developments in SEC rulemaking and enforcement, the impact of Supreme Court actions on the regulatory environment, and good practices for audit committees in a dynamic era of risk. Members also participated in a simulated cybersecurity incident, led by EY and Microsoft.

Members were joined by guests Elad Roisman, partner at Cravath, Swaine & Moore LLP and former commissioner and acting chair of the US Securities and Exchange Commission (SEC), Michael Arnold, partner at Cravath, Swaine & Moore LLP, and Jeffrey Wall, partner at Sullivan & Cromwell LLP and former acting solicitor general of the United States.

A separately published *Board Briefing* will address the corporate diversity, equity, and inclusion (DEI) issues raised in the Supreme Court section of this document. Forthcoming *ViewPoints* will provide additional detail on the audit committees in a dynamic era of risk and cybersecurity discussions.

For a list of meeting participants, see Appendix 1 (page 10).

This *Summary of Themes*[1] provides an overview of each discussion:

EY Building a better working world

SEC developments

Mr. Roisman and Mr. Arnold joined members to discuss the SEC's rulemaking and enforcement. The Commission has issued 47 rules in Chair Gary Gensler's first 850 days in office, a far greater pace than his predecessors set.[ii] Several themes emerged:

- **Companies should monitor SEC rulemaking.** *"We are in a historically atypical time,"* said Mr. Roisman. *"There is an unprecedented volume and interconnectedness of new rules, and a multitude of new rules being issued that do not cover only one subset of SEC registrants or industries. Attention to the new rules is essential, even if companies do not believe a rule will have a direct impact on them, because there may be unintended and indirect consequences of their interactions,"* he advised.
- **The SEC continues to drive enforcement.** SEC enforcement activities have not slowed down. *"Two thematic areas stand out: ESG and cyber,"* Mr. Arnold said, explaining that *"when the current SEC came into office, they established an ESG enforcement task force. When there is a task force like this, there is naturally a pressure for the task force to bring cases in the area to be successful."* He expects an increase in enforcement activities as the new cybersecurity rules take effect and the SEC broadens its focus from procedures and controls around cybersecurity toward compliance with the new rules. *"The focus will be on both the controls around decisions about materiality of the incident as well as the actual disclosures,"* he said.

  Mr. Arnold said that Artificial Intelligence (AI) could soon become a focus area. In the absence of rules about specific disclosures around the use of AI, he encouraged members to balance keeping any disclosures about AI risks as broad as possible *"to help alleviate potential risks that could come with providing information that is too specific with the desire of the SEC and investors to avoid generic, boilerplate disclosure."*
- **The SEC is emphasizing the role of gatekeepers.** Mr. Arnold highlighted the SEC's focus on the role of gatekeepers, including audit committees, auditors, and lawyers. *"The role of gatekeepers is evident in some of the new and proposed rules, for example, with assurance on the climate disclosures,"* Mr. Roisman explained, *"Sometimes the rulemaking is filling a void for a bill that cannot be passed by Congress. The SEC tries to fill the void and then relies on gatekeepers, who are in a position of trust, to fill any gaps."* He does not expect this strategy to change under the current regime, which is sharply focused on issues it perceives in the capital markets, including weakened competition, insufficient investor protection, and markets that do not operate as efficiently as they should.
- **The SEC's proposed rules face more public challenges.** *"In the past, people were more reluctant to challenge a regulator on rules, and there was little legal*

challenge to what was being proposed. But now we are seeing more legal challenges, such as to the SEC's share repurchase and proxy rules. It is also expected that there will be challenges to new rules, including the new climate rules once they are finalized," Mr. Roisman said.

- **Corporate responses to SEC consultations are critical.** Mr. Roisman emphasized the importance of companies—whether directly or via trade associations or other groups—responding to and commenting on the SEC's proposals. The SEC is required to consider every comment in their rulemaking activities, he explained. Decisions about final rules have to be informed by any information that has been submitted, especially where a problem with a rule has been identified, and recent legal precedent has reinforced this.

Members and guests discussed new and proposed SEC rules:

- **Cybersecurity.** Boards should ensure that policies and procedures are designed with the new rules in mind and to *"get the disclosures right,"* Mr. Roisman advised. This will also aid companies in the event of cyber incidents and help if there is a future SEC enforcement investigation. He encouraged boards to participate in cybersecurity tabletops or practice exercises to help detect any gaps in their companies' processes. Some members said their boards have undertaken such simulations, while others have not. One described takeaways from a recent simulation: *"It is important to have a business impact assessment at a detailed level to help with materiality determination; the messaging needs to be controlled because it is always leaked by vendors or employees anyway; and regardless of the four-day rule, it's important to have solid policies and procedures in place that can be followed to help navigate through the incident."*

  Mr. Arnold identified challenges around the cyber rules:

  - **Requesting notification delay in the event of public safety or national security risks.** The current rule provides a 30-day extension if disclosure would create a substantial risk to national security or public safety, but this requires the approval of the Attorney General of the United States.[iii] SEC Commissioner Hester Peirce, in a dissent from the final rule, noted that "obtaining approval within four days will be quite a feat."[iv] Mr. Roisman noted additional guidance for companies would be helpful, *"We're hoping the SEC will provide more clarity on how to obtain the 30-day extension."*

  - **Making the materiality determination.** *"It is important to clarify who makes the materiality determination, how they obtain any relevant information about the cyber incident, and how and when they come together,"* Mr. Arnold advised. He also emphasized the importance of understanding in advance the factors that will be used to guide the materiality determination, noting that the facts and circumstances of the incident will drive those factors that are used.

- **Cyber incidents at third-party service providers.** Mr. Arnold emphasized the importance of understanding when a cyber event at a third-party service provider could be material and require disclosure. He encouraged consideration of current agreements with the third-party and relevant clauses that would help the company obtain the relevant information needed from the third-party to make the required disclosures.
- **Issuing a Form 8-K to minimize risks.** Members questioned whether, out of an abundance of caution, it is prudent to issue a Form 8-K even while a company is still determining whether a cyber incident is material or not. Members voiced concerns that this could set a precedent they would later regret. Mr. Roisman acknowledged the concerns, but predicted that many companies may err on the side of caution and opt to file 8-Ks concerning cyber incidents. He highlighted the high-level nature of the information required for the disclosures, explaining that the information required to be disclosed would often be publicly accessible elsewhere. But he cautioned members that *"over time, the content and accuracy of the disclosure would become more important to help investors understand the impact in light of many Form 8-K disclosures."*

- **Proposed climate-related disclosure rules.** Mr. Arnold predicted that the rules would be finalized in the near future, and that they are likely to maintain the requirements for Scope 3 disclosures at least for some companies. But he added that a number of factors could slow the process down or force changes to the original proposals would be made.

Mr. Roisman concluded by emphasizing the need for companies to be prepared: *"Things may not go the way you want, but you have to be realistic about it. Preparation by management and the board is key. That will serve you well."*

The Supreme Court and the administrative state

Members discussed the regulatory environment with Mr. Wall. Recent and upcoming Supreme Court rulings signal the Court's interest in curbing the power of federal administrative agencies such as the SEC. Members were especially interested in potential effects on the SEC's proposed climate-related disclosure rules. Mr. Wall highlighted several actions that may have an impact:

- **Recent Supreme Court decisions indicate the Court's dislike of administrative power.** Multiple factors have led to a shift in the Supreme Court's views on federal administrative agencies over the past several decades and the current Court is *"more skeptical of government power,"* Mr. Wall observed. Simultaneously, many of these agencies are becoming increasingly ambitious in their agendas. *"This has fueled an environment where fundamental questions that have not been up for debate for decades are now on the table, like how much deference to give federal*

administrative agencies and how much power is too much for those agencies," Mr Wall said. He highlighted two important administrative law developments:

- **Chevron deference.** This doctrine gives federal administrative agencies wide scope to interpret legislative ambiguities. Chevron deference has been in decline in recent jurisprudence, and the Court has now agreed to hear *Loper Bright Enterprises v. Raimondo,* a case that could further erode judicial deference to agencies.[v]
- **Major questions.** Established in a 2022 case, the major questions doctrine "considers whether agencies are 'asserting highly consequential power beyond what Congress could reasonably be understood to have granted.'"[vi] It specifies that "administrative agencies must be able to point to clear congressional authorization when they claim the power to make decisions of vast economic and political significance."[vii] The doctrine could trigger additional regulatory challenges and Mr. Wall noted that it is a *"game changer for those who litigate against an agency over high-stakes matters."*

- **Legal challenges to agencies by corporations and trade associations are increasing.** Some companies and trade associations have not been likely to sue an agency, *"but that is changing for a lot of different reasons, and they now have a better chance at being successful,"* Mr. Wall explained, *"even in spaces where historically no one has sued regulators."*

What should boards consider when determining whether to take a federal administrative agency to court?

Challenging an agency in court is a significant step for a company and an aspect of legal strategy that gets elevated to the board—for example, if a company considers challenging a regulatory finding or an antitrust decision. *"Do you really want to take the government on with those kinds of things? How would you advise boards to think about this?"* a member asked. Mr. Wall recommended boards and management teams consider several factors: *"How existential is the risk? What power is being claimed and how much money is involved? What is your likelihood of prevailing? And what else do you have in front of that regulator that could potentially go south—is there anything else bigger in the fire?"*

- **Challenges to the SEC's final climate-related disclosure rules are likely, but companies still need to begin efforts to comply.** While litigants might use multiple arguments to attack the SEC's rules, in Mr. Wall's opinion the major questions doctrine is the most likely. Opponents could invoke the doctrine to argue that regulation of climate-related disclosures is too significant a question for the SEC to address without clear Congressional authorization. *"It is hard to see how the SEC*

could point to anything that Congress has enacted that clearly says the SEC should be regulating climate policy," he said. He expects legal challenges to the rules to happen quickly: *"I don't think you'll have to wait years in litigation. We should know within the first few months whether the circuit courts or the Supreme Court will issue a stay."* It is nonetheless important for companies to continue to prepare for compliance with the new rules, Mr. Wall said, echoing a theme members heard from Mr. Roisman.

- **California's climate disclosure regulations create new complications.** Most ACLN companies do business in California and will be subject to the state's recent climate legislation, which will require expanded climate-related disclosures. Beginning in 2026, covered entities will be required to publicly disclose Scope 1 and 2 emissions, with Scope 3 emissions disclosed beginning in 2027.[viii] The California law will not be affected by the SEC's final climate rules. *"We are getting ready to comply whether the SEC specifies Scope 3 or not, because we sell in California,"* a member said; *"The only thing you can do is hope that the level of fines may be less because it isn't the SEC fining the company."*

  Mr. Wall explained: *"California's climate law is even broader than the SEC's proposed rules in some ways. If the SEC's climate rule is successfully challenged on the basis that Congress has not given the SEC power to regulate climate policy, then a natural conclusion is that it is left to the individual states."* He added, *"This Supreme Court is pretty receptive to arguments of state power and skeptical of federal preemption of state law. It leaves a lot of room for 'red' and 'blue' states to make things difficult for companies."* A scenario of state-led legislation on climate disclosures could be problematic, said a member: *"The worst thing that can happen is to have 50 of these sets of climate rules that you have to comply with."*

Mr. Wall also discussed how companies may be affected by the recent Supreme Court ruling on affirmative action in colleges and universities. A report on this will be shared in a separate Tapestry Networks *Board Briefing*, "Boards face new scrutiny on diversity, equity and inclusion programs."

How audit committees are evolving in a dynamic era of risk

Large, global companies face risks that are increasingly complex and interrelated. This members-only session explored how audit committees, charged with risk oversight, are adapting their approaches. Members described good practices their audit committees and boards employ to oversee risk:

- **Ensure that oversight responsibilities are appropriately delegated within the board.** *"As audit chairs, our response should not be to just take everything on. I think*

we need to identify each key risk, how it impacts our company, and ensure it gets on the board's agenda. Too many times, audit committee agendas expand because everyone thinks new risks or issues need to go to the audit committee. But that is not necessarily right, nor does it serve the shareholders properly," one member said. As an example, several members said that their audit committees play a role in overseeing controls over AI, but that other aspects of the technology and its usage should be a full board discussion. To delegate risk oversight, some members use a mapping process that identifies key risks and clearly designates oversight of each of these risks to the full board, the audit committee, another committee, or a subcommittee.

> **"There is a New York Stock Exchange requirement that audit committees own risk management, but that doesn't mean we own all risk."**
>
> *- ACLN Member*

- **Coordination and communication among committees is critical.** Members described several good practices, including frequent communication between committee chairs. *"We interact at the chair level a lot. We make sure nothing is falling through the cracks,"* one said. Several reported having overlapping committee members, which helps ensure information flows clearly and frequently between the committees. In one company, committee chairs all sit on the Compensation Committee, *"since all roads and risks essentially lead to compensation."* Joint sessions of committees dealing with risks, especially those with elements impacting multiple committees—such as ESG—can also be beneficial.
- **Be intentional about horizon scanning and planning for black swans.** Identifying emerging and unknown risks is inherently challenging. One member described how she thinks about this challenging task: *"You are not trying to forecast. Think of it more in terms of the many realities that could happen. Then create an envelope of those possibilities. You have to accept that you will miss things on either side of the envelope, but also accept there's a lot of resource that can get burned trying to deal with things outside of it."* She added, *"The question I ask is: What would a reasonable person on a jury have expected you to do? That's the envelope you want to worry about."* A process for identifying new risks is vital. Members shared how they identify "black swan" risks, including consulting a futurist and using a cross-functional risk team that begins each quarterly meeting with a discussion on emerging risks.
- **Tightly manage audit committee agendas to allow adequate time for risk conversations.** Members described practices for managing crowded audit committee agendas, such as holding premeetings with management and using executive sessions. One described *"immersion sessions,"* where the committee *"takes topics outside of the audit committee meeting so we can delve into them*

further and spend enough time on them." Another explained how she changed management's approach to premeeting materials: *"We started being far more disciplined in having management not present information in the preread. Instead, we say that it should be taken as read and we ask management about areas of concern. It was really hard to do, but worth the effort and easily frees up 30-45 minutes of time in our meetings."*

Could committee members defer too much to the audit chair?

Members said that they do extensive preparation for each audit committee meeting to ensure agendas and time are managed efficiently. But one raised a concern: *"I'm doing so much offline and outside of meetings that I worry at times that as much as I try to bring committee members in, I'm sensing a real willingness to defer to the audit chair. For example, I may be comfortable on a certain topic because I've spent two hours discussing it with management and others beforehand, but I'm not sure how the rest of the committee could be comfortable with it. I worry that I'm a one-man band to some extent."* This concern resonated with other members.

A forthcoming ViewPoints will provide additional detail on how audit committees are evolving to address the complex risk environment, including insights from a recent meeting of the European Audit Committee Leadership Network.

Cybersecurity simulation

Members participated in a simulated emergency board meeting of XtraEnergy, where they learned the fictious company was the victim of an ongoing cyberattack. ACLN members played the role of XtraEnergy board members, and leaders from EY and Microsoft played the roles of chief executive officer, chief information security officer, general counsel, and external auditor.

In the debrief that followed, EY facilitators noted that while teams wanted more information about the incident and the circumstances surrounding it, the reality is that hard decisions must often be taken on the basis of very limited data. They also pointed to the line that separates the board from the management team: in times of crisis, boards may need to significantly increase its support and oversight, but executives must continue to run the company.

Members benefitted from earlier discussions on the new SEC disclosure rules and considered the need for early incident disclosures in a Form 8-K, among other communications. One of the key factors identified was immediate communication with almost every interested party: investors, regulators, government agencies, and relevant

authorities, staff, and customers. Additional key takeaways include:

- **Ensure that crisis plans are regularly practiced and updated.** Developing comprehensive, mutli-scenario crisis plans is necessary but not sufficient. The plans must be regularly drilled, reviewed, and updated. One member explained, *"Having a plan is the starting point. Drilling robust scenarios won't prepare you for everything but gives you some muscle memory."*
- **Crisis plans should include detail about communications, including who and when.** Details for both internal and external communications should be included in plans. Importanlty, they should include not only content but mechanics (e.g., using satellite phones when voice-over-IP phones are disabled). As one member said, *"If you can connect with each other, you can figure it out. But if you can't communicate, you are dead in the water."*
- **Consider involving law enforcement early.** A member had recently attended an event where FBI Director Chris Wray laid out numerous reasons for engaging law enforcement early in any cyberattack; he pointed to the Bureau's experience with cyber aggressors, and its interest in shutting down their criminal networks.
- **Clarify and understand ransomware policies.** Boards should be clear about who has the authority to authorize payment of ransomware and have confidence in the decision process. Clarity about the company's cyber insurance coverage and any limitations also need to be taken into account.
- **Supporting leaders through the crisis is critical.** Boards should remember that any business crisis generates significant mental stress and should be prepared to support leaders who may "crack under pressure." But crises can also reveal emerging leaders. One member noted that his company's current CEO was selected because of the way she had stepped up during the COVID-19 pandemic, earning her position.

A detailed review of lessons learned from the simulation, questions for boards to consider, and additional cybersecurity oversight good practices will be shared in an upcoming ViewPoints.

Appendix 1: Participants

The following members participated in all or part of the meeting:
Fernando Aguirre, Audit Committee Chair, CVS Health
Joan Amble, Booz Allen Hamilton
Jeff Campbell, Audit Committee Chair, Aon
Ted Craver, Audit Committee Chair, Wells Fargo
Bill Easter, Audit Committee Chair, Delta Air Lines
Lynn Elsenhans, Audit Committee Chair, Saudi Aramco
Tom Freyman, Audit Committee Chair, AbbVie
Bella Goren, Audit Committee Chair, General Electric and Marriott International
Gretchen Haggerty, Audit Committee Chair, Johnson Controls
David Herzog, Audit Committee Chair, MetLife
Akhil Johri, Audit Committee Chair, Boeing and Cardinal Health
Dagmar Kollmann, Audit Committee Chair, Deutsche Telekom*
Paula Price, Audit Committee Chair, Accenture and Warner Bros. Discovery
Tom Schoewe, Audit Committee Chair, General Motors and Northrop Grumman
Cindy Taylor, Audit Committee Chair, AT&T
John Veihmeyer, Audit Committee Chair, Ford

The following members participated virtually in all or part of the meeting:
Janet Clark, Audit Committee Chair, Texas Instruments
Pam Craig, Audit Committee Chair, Merck
Dan Dickinson, Audit Committee Chair, Caterpillar
Charles Holley, Audit Committee Chair, Amgen and Carrier Global
Arjun Murti, Audit Committee Chair, ConocoPhillips
Jim Turley, Audit Committee Chair, Citigroup
Maria van der Hoeven, Audit Committee Chair, TotalEnergies*

EY was represented by the following in all or part of the meeting:
Julie Boland, US Chair and Managing Partner and Americas Area Managing Partner, EY
Dante D'Egidio, Americas Vice Chair – Assurance, EY
Pat Niemann, Partner, Americas Center for Board Matters, EY

Tapestry Networks was represented by the following in all or part of the meeting:
Jonathan Day, Chief Executive
Bev Bahlmann, Principal
Todd Schwartz, Principal
Kelly Gillen, Associate
Abigail Ververis, Project and Event Manager
Ashely Vannoy, Project and Event Manager

**Member of the European Audit Committee Leadership Network*

Endnotes

[1] *Summary of Themes* 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. Quotations in italics are drawn directly from members and guests in connection with the meeting but may be edited for clarity.

[ii] Committee on Capital Markets Regulations, "The Unprecedented Pace of SEC Proposed and Final Rulemakings Continues," August 31, 2023.

[iii] Cravath, Swaine & Moore LLP, "SEC Adopts Cybersecurity Disclosure Rules for Public Companies," memo, August 1, 2023.

[iv] Hester M. Pierce, "Harming Investors and Helping Hackers: Statement on Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure" (statement, Washington, DC, July 26, 2023).

[v] Sanne Knudsen, "Three-Minute Legal Talks: Loper Bright Enterprise v. Raimondo," video interview by Three-Minute Legal Talks, *University of Washington School of Law*, October 23, 2023.

[vi] Kevin A. Akrong, "FTC Proposes to Ban Non-Compete Agreements, and Takes First-Ever Enforcement Actions Against Companies for Imposing Non-Compete Terms on Workers," Cravath, Swaine & Moore LLP, January 6, 2023.

[vii] Akrong, "FTC Proposes to Ban Non-Compete Agreements, and Takes First-Ever Enforcement Actions Against Companies for Imposing Non-Compete Terms on Workers."

[viii] Sullivan & Cromwell LLP, "California Enacts Expansive Climate-Related Disclosure Laws," memo, October 12, 2023.