tapestry NETWORKS

ACLN SUMMARY OF THEMES

Geopolitics, regulatory agendas, cybersecurity, and digital currencies

June 2026

On June 2 and 3, 2026, members of the Audit Committee Leadership Network met in Washington, DC. Topics included:

- **Conversations with SEC Chairman Paul Atkins and SEC Chief Accountant Kurt Hohl**
- **Cybersecurity discussion with the FBI** with Brett Leatherman, Assistant Director of Cyber Division and Kristin Grimes, Chief, Cyber Law Unit
- **Navigating geopolitical uncertainty** with Steven Weber, Partner at Breakwater Strategy
- **US-China competition** with Evan Medeiros, Penner Family Chair in Asian Studies at Georgetown University and Andrew Polk, Co-Founder and Head of Economic Research at Trivium
- **Quodlibet (members' choice)**
- **Stablecoins and their use in global companies** with Brendan Maher, Partner/Principal at EY and Jai Massari, Of Counsel, Arktouros

For a list of meeting participants, see Appendix 1 (page 9).

This *Summary of Themes*[ii] provides an overview of the following discussions:

EY Shape the future with confidence

Conversations with SEC Chairman Paul Atkins and SEC Chief Accountant Kurt Hohl

Members met separately with SEC Chairman Paul Atkins and Chief Accountant Kurt Hohl for two sessions covering SEC priorities. The conversations focused on the Chairman's well-publicized "Make IPOs Great Again" agenda and the Commission's "ACT" approach to reform efforts: advancing regulatory frameworks, clarifying the boundaries and application of overlapping regulatory regimes, and transforming disclosure requirements to focus on materiality. Members discussed the prospect of making reforms durable, the trend of reincorporating outside of Delaware, international regulatory alignment, the role of proxy advisors, and striking the right balance to encourage innovation in AI and digital assets while upholding the SEC's core missions of investor protection, maintaining efficient markets, and facilitating capital formation.

Cybersecurity discussion with the FBI

As cyber threats grow in sophistication, directors face mounting pressure to move beyond high-level awareness into substantive engagement with cyber risk. Regulatory scrutiny of board oversight is intensifying, and clear approaches to address cyber incidents are on the agenda. Brett Leatherman, Assistant Director of Cyber Division and Kristin Grimes, Chief, Cyber Law Unit at the FBI joined members to discuss the importance of cyber resilience, highlight the new threats on the horizon, and underscore the importance of the quality of a company's response to a cyber incident.

Several themes emerged during the session:

- **Organizations where boards engage with cyber risk are more resilient.** Directors must ask questions around threat exposure, defensive posture, and whether the CISO has adequate authority and resources. *"The concern that we have is that there is not enough dialogue happening between boards and management,"* Mr. Leatherman told members, *"Organizations that take risk seriously at the board level respond a lot quicker to cyber breaches"*. Ms. Grimes pointed out the cultural dimension: *"Certain organizations view this as a compliance checkbox — it needs to be a conversation around best practices instead."*
- **The technology threat environment is evolving**. AI is vastly accelerating offensive cyber capabilities. *"Most organizations are still defending against cyber threats at human speed,"* Mr. Leatherman observed, *"cyber exploitation methodology is going to get better and better, and AI agents are going to start*

Quantum and cyber

Quantum computing threatens the cryptography that underpins most enterprise security. Malicious actors are collecting encrypted data today against the day quantum systems can break it; companies therefore need to act now. Fortunately, quantum-resistant encryption can be done with conventional computing.

working around the clock." Attack surfaces have shifted; the primary point of infiltration is exploitation of edge infrastructure — firewalls, VPNs, and network appliances. *"2025 was the year of edge device exploitation, 2027 is the same but at scale,"* Mr. Leatherman warned.

- **Companies are still failing to engage with the FBI in advance of a breach**. *"There are zero instances of an organization coming to the FBI and later saying 'what was I thinking' — so many people instead think 'why did I not do this earlier.',"* Mr. Leatherman told directors, *"Days matter with this stuff, and with AI, days matter even more,"* FBI field offices participate in tabletop exercises, share threat intelligence in advance of incidents, and help organizations navigate the disclosure requirements immediately after a breach. Further, that relationship is legally protected. *"Anytime you share cyber information with us, it receives protections and under the Cybersecurity Information Sharing Act of 2015, receives additional protections including and maintaining the privilege that was attached to that information,"* Ms. Grimes explained. Companies should reach out to the FBI today to build that relationship.
- **Crisis response should be pre-authorized, not real-time**. When a cyber incident occurs, boards must have a plan in place to act quickly. *"We can't prevent breaches anymore, but we can work to respond quickly,"* Mr. Leatherman told members. He also shared the FBI's view on ransomware: *"We usually advise to not pay the ransom. You are trusting the bad guy to get you out of a problem, and what we see time and time again is that they're not deleting your data."* Cyber insurance adds further uncertainty: *"Cyber insurance is constantly changing, including more exclusions resulting in denials,"* Ms. Grimes said. Given the volatility of coverage terms, members noted that general counsel should review a cyber insurance policy in detail every time it is renewed.

Navigating geopolitical uncertainty

Global companies are no longer operating in an environment where government is a background condition to be monitored and managed. Steve Weber, Partner at Breakwater Strategy, argued that the US administration is driving a structural change in the relationship between government and business — one that demands a fundamental rethink of how boards assess risk, engage with regulators, and make strategic decisions.

Key themes from the discussion included:

- **The government has become an active market player, not just a regulator.** Mr. Weber identified the emergence of 'the mercantile state': "*A government that is now an active player in markets as well as a referee. It sees itself as having its own P&L, and uses regulation and oversight aggressively to bolster its own position."* The implications for boards are direct: *"It's not plausible for boards to think about doing*

their jobs as if the government's primary tools are taxation and antitrust regulation — now they are using equity stakes, contract blacklisting and favoring, incentivized purchases and divestitures."

- **The administration's governing philosophy is anti-managerial and pro-disruption.** *"This administration's end game is not freedom of action for corporates, what we have is a broader project of societal transformation,"* Mr. Weber told members. The specific flavor of that project matters for how boards interpret signals from Washington: *"The relevant point here for corporates is to see this philosophy as anti-managerial, anti-bureaucracy, opposed to concepts like risk aversion — focused on the idea that all that stuff has sucked out important energy that makes American business and American society great."* The implication is that uncertainty is not a byproduct of this administration's approach but rather an intentional feature.
- **AI is the fulcrum around which the administration's economic and geopolitical strategy is organized**. *"The government is placing a generational bet on AI productivity and advantage,"* Mr. Weber told members, *"The government wants you to deploy and spend aggressively to bring in a technology revolution."* The urgency is driven explicitly by competition with China, but there is a growing gap between the administration's framing of AI as a national security imperative and the public's experience of AI as a job threat. *"The China threat around AI is very abstract for most people and very hard to measure vs something so tangible like 'I'm going to lose my job.'"*

US-China Competition

The US-China relationship sits at the center of many strategic questions facing global companies today. Evan Medeiros, Penner Family Chair in Asian Studies at Georgetown University, and Andrew Polk, Co-Founder and Head of Economic Research at Trivium China, discussed with members where the relationship stands and what it means for companies navigating an increasingly complex operating environment.

Mr. Medeiros and Mr. Polk discussed several topics:

- **Companies are caught in a difficult bind**. *"Companies are being put in a situation where at some point they will either be compliant with Chinese law or compliant with US law,"* Mr. Polk said. China is actively reinforcing this bind: *"China is bringing out counteractive measures — blocking rules and other mechanisms — and pushing back against any actor that is supporting foreign governments in pursuing economic coercion against China."* On data privacy and security specifically, the situation is unlikely to improve soon. *"I don't think it's going to change materially in 4/5 years,"* Mr. Polk said.
- **Supply chain exposure runs deep**. *"All companies have chokepoints, they often emanate from third- or fourth-tier suppliers,"* Mr. Polk explained. Further, China is

already moving on to the next generation of dependencies: *"The US is looking at the current chokepoints while China is trying to build out the next dependencies — they are looking at frontier and emerging industries."*

- **The political risk of doing business in or with China is intensifying.** *"The big issue here is that your relationships with Chinese institutions get scrutinized by the US government, especially the Congress"* Mr. Medeiros noted, pointing to the public criticism of major US banks for their involvement in Chinese IPOs. The definition of which Chinese counterparties are off-limits is also shifting — moving beyond defense-linked entities into technology and AI. *"The Pentagon is adding Chinese companies to its sanctions list not because of any clear connection to the Chinese military but because they are involved in the AI buildout in China – their rationale is that the US wants to compete with China in the AI race and own the full technology stack,"* Mr. Polk observed.
- **Cyber-enabled economic espionage is a company risk.** *"They break into your records and get info and sell it into Chinese SOEs — are there protocols for how to deal with your staff that's in China? People going to China? If there is a material breach to your network it needs to be reported to the SEC,"* Mr. Medeiros told members.
- **Boards cannot plan around the current stability**. The surface calm in the US-China relationship right now and for most of 2026 should not be mistaken for durability. *"There is now a veneer of stability and of communication and understanding but I don't think there's a lot of substance to it,"* Mr. Medeiros said, *"It's very likely that within the next 12 months, we will snap back to a much more competitive approach — I worry about a future trade war that will be much tougher than in 2025."*

Quodlibet (members' choice)

In a breakfast discussion, members raised topics that have been front of mind: the practical implications of quarterly reporting reform, cybersecurity tabletop exercises, audit and compensation committee coordination, PCAOB audit quality, and the use of AI by auditors.

Several themes emerged from the discussion:

SEC

- **Most companies expect to keep reporting quarterly regardless of what the SEC permits.** Regulatory changes may be coming, but investor expectations, competitive dynamics, and internal discipline are likely to keep most large companies on a quarterly cadence. *"We wouldn't change anything due to investor expectations — we still report quarterly, otherwise it would be a competitive disadvantage,"* one member

said. *"We give guidance every quarter and I can't imagine that changing — it would be nice to eliminate the costs but the analysts are insatiable,"* added another.

- **Durability is the concern.** The effort required to shift to semiannual reporting would be substantial, and unwinding that change if the regulatory environment shifted again under a future administration would be equally costly. The cost implications of changing disclosure cadence — and then having to reverse course — were seen as a more significant risk than the cost of continuing to report quarterly

Cybersecurity

- **Tabletops are valuable, but are not universally adopted.** *"We're better for having done it. It's important to have communication plans, escalation and decision rights and clarity around all that in a moment of moving quickly and in a crisis,"* one said. Several others, while recognizing the benefit, sounded a note of caution, citing the possibility of providing a litigation roadmap in the event a tabletop exercise were to reveal an unidentified weakness.
- **Modalities vary.** Some members stated that exercises on a surprise basis are more useful than planned ones. *"You got a real sense of the bottlenecks time-wise, and we had to devise plan B's."* A member who had lived through a real incident offered a caveat: *"in a lot of cases the involvement on the board is occurring over a matter of a week or more — that's hard to simulate in a tabletop."* The emerging consensus was that every director should understand escalation procedures, decision rights, and communication plans before they are needed – whether or not they participate personally in a tabletop exercise.

PCAOB

- **Inspections generated limited value for audit committees.** Members found recent PCAOB engagements heavily focused on individual engagements rather than firm-wide audit quality and process. There was limited interaction between the PCAOB and the audit committee chairs, who noted that inspection findings produced little that they could act on. *"There is a lot of value lost to us as audit committees, these inspectors have seen a lot of different companies and files and processes — but it all gets lost."* They found the feedback loop too slow, too filtered, and insufficiently specific. *"It might be helpful for the PCAOB to provide information on a more timely basis,"* one member said, *"Hearing a debrief on what happened as opposed to just 'we got a pass' — I think that would be more valuable,"* added another.

Executive Compensation

- **Interlocking committee membership is a common approach for audit-compensation coordination. "***The comp chair sits on my audit committee, and a member of the audit committee also sits on the compensation group,"* one member

noted, a structure several others confirmed.

- **Non-GAAP adjustments raise concerns for both committees.** A significant coordination point is on ensuring consistency between what gets excluded for financial reporting purposes and what gets used for compensation calculations. *"We compare notes on any non-GAAP adjustments. Yes, they're being adjusted for financial reporting, but there could be something that is highly unusual and we think the management team's incentive pay should reflect that."*
- **Clawbacks add a layer of complexity.** Clawbacks require further coordination between the two committees, particularly when restatements are involved. The audit committee's role becomes more significant when earlier awards must be recovered, and process clarity between committees is essential.

Stablecoins and their use in global companies

Until recently, stablecoins sat at the periphery of corporate finance and were associated with crypto trading and use outside the United States rather than mainstream financial operations. That is changing. Brendan Maher, Partner/Principal at EY, and Jai Massari, Of Counsel at Arktouros, made the case that the passage of the GENIUS Act gives stablecoins a legal framework to make them a legitimate form of digital money.

Stablecoins are a fundamentally different kind of money

Ms. Massari distinguished credit money, which is at the same time an asset of the holder and a liability of another party, from non-credit money, such as a gold coin. In her view, GENIUS-regulated stablecoins are designed to be non-credit money. *"Regulated stablecoins are standardized stable assets — electronic cash. We don't care who the issuer is."* The practical implication is that a GENIUS-regulated stablecoin issued by a large bank and one issued by a non-bank payment provider should be economically equivalent — a significant departure from the current environment where the creditworthiness of the issuer matters. “This is also the first money transaction where individual payment transactions can clear and settle without ever touching a bank,” she told members, *“All of a sudden you have this instrument where the banks are not involved at all. They are losing their payment monopoly."*

Mr. Maher and Ms. Massari discussed implications for boards:

- **The GENIUS Act has given stablecoins new relevance.** *"Up until the last six months I would have said that companies didn't need to pay attention to stablecoins because they didn't have the legal frameworks,”* Ms. Massari said, *“Today I think they will be good forms of money once GENIUS is enforced in the US."* The GENIUS

Act establishes a regulatory framework under which stablecoin issuers are subject to prudential oversight, reserve requirements, and special bankruptcy protections that ensure holders get their money back quickly if an issuer fails.

- **The most immediate use cases are treasury and cross-border payments**. Ms. Massari identified treasury payments among corporate affiliates, particularly cross-border, as the most immediately relevant use case. Mr. Maher pointed to a related opportunity around treasury management: *"Those business reasons where we need to be able to move cash outside of operating hours, that can be done with stablecoins."* The programmability of blockchain-based instruments opens further possibilities — automated payment flows, collateral management, and AI-integrated treasury functions — though Maher was clear that *"When you think about it as a payment instrument, that's where you start to see some of the benefits."*
- **The risks are real and boards need to understand them**. Cybersecurity risks are the most immediate. *"When you get back to the concept of private keys and where those are managed and stored, there's an operational risk there,"* Mr. Maher said. Further, the legal infrastructure for handling payment disputes does not yet exist in a mature form: *"Today we don't have a good set of standards for stablecoin transactions,"* Ms. Massari noted. And the concentration of power in issuers, who have the technical ability to freeze or destroy tokens, creates their own governance questions. In this regard, stablecoins have some similarities to traditional payments, where banks have control over funds in the accounts they control, but in different configurations where the issuer has control over the global supply of stablecoins.
- **The timeline for adoption remains unclear.** While not distant, mainstream corporate relevance is not fully here yet. *"Today no, we're early. But you should start to pay attention because you're going to start seeing a variety of solutions using stablecoins. It will probably take at least a year because you need GENIUS regulated stablecoins to be up and running and then you need banks to support stablecoin wallets. But then I think yes — there's enough juice to squeeze*," Ms. Massari told members.

Appendix 1: Participants

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

Judy Bruner, Applied Materials

Jeff Campbell, Aon and Marathon Petroleum

Christine Catasta, Erste Group Bank (EACLN member)

Dave Evans, Cardinal Health

Laura Hay, MetLife

Bob Herz, Morgan Stanley

Joe Householder, AMD

Lori Lee, Emerson Electric

Jennifer Li, SAP (EACLN member)

Amity Millhiser, The Coca-Cola Co.

Leeny Oberg, Adobe

Kimberly Ross, Cigna

Tom Schoewe, Northrop Grumman

Tom Sweet, 3M

Dessi Temperley, Coca-Cola Europacific Partners (EACLN member)

Doug Terreson, Phillips 66

Pat Yarrington, Lockheed Martin

Tracey Travis, Accenture

EY was represented by the following in all or part of the meeting:

Julie Boland, EY Americas Area Managing Partner and EY USLI Regional Managing Partner

Dante D'Egidio, EY Americas and US Managing Partner and CEO-elect

Jennifer Lee, Managing Director, Americas Center for Board Matters

Pat Niemann, Partner, Americas Center for Board Matters Leader

The following Tapestry Networks representatives participated in all or part of the meeting:

Dennis Andrade, Managing Director

Jonathan Day, Chief Executive

Laura Koski, Project and Event Manager

Jo Rhoden, Executive Director

Ginevra Rollo, Associate

Todd Schwartz, Executive Director

Jason Watkins, Managing Director

Endnotes

[i] Use of Artificial Intelligence: Portions of this document may have been prepared with the assistance of artificial intelligence tools. All content has been reviewed and approved by Tapestry Networks.

[ii] *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.