VIEWPOINTS

Beyond AI: new technologies on the horizon

July 2026

The topic of artificial intelligence has come to dominate conversations about technology to an extent that few non-experts would have predicted a mere five years ago. But even as boards and management teams come to terms with the risks and opportunities of AI, a collection of new technologies is already emerging. These technologies—neither strictly offshoots of AI nor entirely independent of it—are likely to reshape business just as much as AI has done over the past three years.

In June 2026, ACLN and ACN members gathered in Washington, DC, along with guest experts, for a series of discussions about three of these emerging phenomena: quantum computing, AI-enabled cyber threats, and stablecoins. This *ViewPoints* explores the governance challenges that these advances pose.

For a list of reflection questions for audit committees, see page 8. For a list of participating audit chairs, see Appendix 1 (pages 10–11), and for guest biographies, see Appendix 2 (pages 12–13).

This *ViewPoints*[1,2] covers key themes that emerged from the meetings and related conversations:

New technologies are on the horizon

AI remains the defining preoccupation of most boardrooms. Its ongoing evolution, competitive implications, and governance challenges have demanded significant attention from boards and management. But new technologies are emerging. Some are shaped by AI, some will boost its capabilities, and some will turn it into a weapon. These growing opportunities and risks will soon demand significant board attention.

Quantum computing

Quantum computing is not simply a faster version of classical computing: it is a fundamentally different way of processing information. While classical computers store and manipulate data as binary bits, quantum computers exploit the properties of quantum mechanics to operate in multiple states simultaneously, enabling them to solve classes of problems that no classical machine can dispose of, regardless of speed. *"It processes data in such a different way than classical computers,"* said Simon Phillips, chief technology officer of Oxford Quantum Circuits (OQC). *"A classical computer can never assimilate that level,"* added Gerald Mullally, OQC's co-founder and chief executive officer. While commercial-scale quantum capability has yet to emerge for most applications, the roadmap is shaping up quickly.

AI-enabled cyber threats

AI continues to reshape the cybersecurity landscape, as it aids and abets behavior-based exploitation. For example, it can chain multiple techniques together without human intervention and generate social engineering at unprecedented levels of sophistication. *"Cyber-exploitation methodology is going to get better and better, with AI agents working around the clock,"* said Brett Leatherman, assistant director of the FBI's Cyber Division. The gap between what attackers can now do and what most organizations are equipped to detect and respond to is today's central cyber-governance challenge.

Stablecoins

Stablecoins are digital assets designed to maintain a stable value relative to a reference currency—most commonly the US dollar—recorded on a blockchain rather than held in a traditional bank account. Their economic structure distinguishes them from conventional deposits: where a bank deposit is an unsecured liability backed by the issuing institution's balance sheet, a regulated stablecoin holds specified liquid reserve assets one-to-one. *"Conceptually and economically, stablecoins should be viewed as non-credit money,"* said Jai Massari, of counsel at Arktouros. *"They are electronic cash."*

Until recently, that distinction was largely theoretical for mainstream companies, but the passage of the GENIUS Act[3] this year changed that. With a new legal framework in the United States, the question of how organizations will interact with this new form of money is moving up the agenda.

AI is an amplifier for both risk and opportunity

Quantum computing, cyber-threat technologies, and stablecoins can be shaped by and intersect with AI. The same capability that makes quantum computing a transformational tool for industry makes it a more

dangerous instrument for adversaries, and the same AI models that enable autonomous financial transactions also enable autonomous cyberattacks.

Across multiple Tapestry discussions, the theme was the importance of understanding AI as a sort of force multiplier running through these technologies:

- **AI has changed the nature of cyber threats.** Cyber actors are moving from static, signature-based attacks that rely on known indicators—IP addresses, file hashes, and behavioral patterns that defenders can learn to recognize—to AI-enabled, behavior-based exploitations that run continuously, adapt continuously, and link multiple techniques together without human intervention. *"In certain lab environments, they are testing with AI models that can exfiltrate data in 25 minutes,"* said Mr. Leatherman, citing Palo Alto's 2026 Global Incident Response Report.[4] *"No human can defend against that."* Where organizations once tracked known indicators, the new environment requires AI-based heuristic detection. *"With AI, we're moving away from atomic indicators to behavior-based detection,"* Mr. Leatherman said. *"If we're not using artificial intelligence to start to detect and block, we're going to be in a lot of trouble."*

Training with AI

As AI-enabled attacks grow more sophisticated, some organizations are using AI to improve their training and awareness programs. *"In one of my boards, they used AI to develop a new phishing campaign throughout the company,"* said a member. *"AI helped take it up two or three notches."* Defending against AI-enabled threats increasingly requires AI-enabled defenses.

- **The controls gap is widening, and audit committees are not yet asking the questions that would expose latent weaknesses.** Most chief information security officers (CISOs) are experimenting with AI-based detection and response tools. *"They are starting to implement,"* said a member, *"but it's probably not at the speed they should be."* The cultural dimension compounds the problem. *"Certain organizations view this as a compliance checkbox; it needs to be a conversation around best practices instead,"* said Kristin Grimes, chief of the FBI's Cyber Law Unit. The FBI's Operation Winter Shield[5] offers a practical starting point for board-level conversations. *"I would leverage AI to drop those controls into a large language model and help me understand how to start having conversations with the CISO,"* Mr. Leatherman suggested. *"Organizations that take risk seriously at the board level are more resilient and respond a lot quicker to cyber breaches."*
- **Quantum and AI are mutually reinforcing.** Some organizations are already using AI to identify where quantum can be applied. *"We are using AI to identify things in the organization that quantum can do better,"* Mr. Phillips told members. But the impact goes the other way too, noted OQC's Mr. Mullally, as quantum computers can generate synthetic data that is *"of life,"* drawing from the underlying physics of complex systems that classical machines cannot replicate. *"The true potential of quantum for AI is efficient data generation,"* Mr. Mullally said. Classical computers are trained on the internet, while quantum computers can generate training data of a fundamentally different quality, with significant implications for AI capability.

- **Stablecoins may become the payment infrastructure for AI agents.** The programmability of blockchain-based payments makes them a natural fit for AI agents that need to transact autonomously, rapidly, and without relying on banking infrastructure built for human-speed operations. *"Some of the most interesting use cases we are seeing today are around AI,"* said Brendan Maher, partner/principal at EY. It is still early—most stablecoin volume remains in crypto-trading activity—but as agentic AI scales inside organizations, the demand for machine-speed, programmable payment infrastructure will scale with it.
- **Strong AI governance enables companies to move faster, and boards play a key role.** With new models and tools *"coming and going at the speed of light,"* as one member put it, boards that make AI governance a priority—ensuring visibility into how data, models, and unstructured assets are managed and holding leadership accountable—give their organizations the clarity to move faster.

Data is at the foundation of technology

Data sits at the center of any technology discussion, and it's a critical focal point for boards and audit committees. The same question resounds across cybersecurity, quantum, and stablecoins: does management know what data the organization holds, how it is protected, and what its lifespan of value is?

Member and guest discussions highlighted the following observations and suggestions:

- **Nation-state actors are stealing and storing data.** Mr. Leatherman and Ms. Grimes discussed with members what the FBI terms *"hack now, decrypt later"* operations, where actors gain persistent access, exfiltrate data, and store it for later use. The threat is not only what adversaries can do with data now, but what they will be able to do with it in the future with the benefit of then-prevailing AI and quantum capabilities. *"The concern is trying to understand what data has already been lost,"* Mr. Leatherman said, *"and what can be done to prepare our environments now."* China, for example, is storing mass amounts of encrypted data with the intention of cracking it when quantum decryption becomes viable.
- **Data risk demands a future focus.** The *"harvest now, decrypt later"* threat is straightforward: hostile actors are collecting encrypted data today with the intention of decrypting it once quantum computing reaches sufficient capability. *"What is the data that is valuable ten years from now? That's the data that is most at risk,"* Mr. Mullally said. For most commercial organizations, the data most at risk is long-lived sensitive material: contracts, personnel records, supplier relationships, legal communications. *"If you lose it now and hostile states gain the capability to decrypt it in the future, they can turn it into intelligence,"* he said.
- **Post-quantum cryptography should be seen as a strategic risk.** The National Institute of Standards and Technology (NIST) and National Security Agency (NSA) have issued recommended algorithms, and quantum-safe encryption can be implemented now across most standard data environments. *"Post-quantum cryptography should be on a list of strategic risks,"* Mr. Phillips said. *"Cryptography that is quantum-safe exists today. You do not need the technology to beat the technology."* The bottleneck is not access to the tools but the absence of a data inventory, one that identifies what needs protection together with a road map for prioritizing it.

Audit your data to know what to prioritize

Organizations cannot protect what they have not mapped, so a data audit is useful in establishing a road map for data protection. Here are three key questions to ask:

- *Where is the data?* Not at the level of broad system categories, but with enough specificity to identify which assets are encrypted and under which standards.
- *How is it encrypted?* Current encryption standards will eventually be breakable by quantum systems, and the question is whether the algorithms in use today are on the NIST and NSA's lists of recommended post-quantum alternatives.
- *What is the lifespan of the data's value?* Legal communications, personnel records, supplier relationships, and strategic plans tend to hold value far longer than organizations may account for.

The output of that audit will provide key indicators on which data to prioritize for re-encryption, which third-party and vendor contracts to revisit, and where the organization's most significant exposure sits.

- **For stablecoins, reserve transparency is a data verification question.** The GENIUS Act requires reserves to be held one-to-one in high-quality liquid assets. But the composition of those reserves—and the accuracy of disclosure—varies between issuers. Audit committees overseeing organizations involved with stablecoin instruments will need to understand that verification means confirming not only that reserves exist, but also that a reserve's actual composition lines up with what it claims to be. *"Today you care very much which stablecoin you hold,"* said Ms. Massari. Unlike a bank deposit, where the creditworthiness of the institution provides a backstop, a stablecoin is only as sound as the assets behind it, making reserve data an important thing for boards to verify.

The pace of change is outrunning governance

"The advent of AI made us realize that transformational technologies appear often, and they appear time and time again." Mr. Phillips told members. *"We discover new things all the time, but there's so much change at the moment that you need to make sure you have the internal bandwidth to feel ready."* New technologies operate on disparate timelines, and the governance challenge is not simply to understand each technology, but to have the capabilities to absorb multiple disruptions simultaneously.

Meeting discussions yielded several key observations:

- **AI-enabled cyber threats expose dated governance processes.** As frontier AI models are released, their ability to identify software vulnerabilities at scale will result in patch volumes that current processes cannot absorb. *"The expectation of these new models is that we won't be able to have the same process around patching,"* said a member. *"We're reimagining our patching process now so that when we get access to these models, we'll be able to do it at greater speed."* Patching is the most immediate governance process to rethink, but it is not the only one. Any governance process that depends on human review at each step—vulnerability triage, access controls, incident

escalation—will need to be redesigned for a world where inputs arrive faster than people can process them.

- **Quantum's commercial road map is closer than most boards realize.** *"I had an epiphany with AI—the speed has been insane,"* said one member. *"I feel the same listening to you right now—quantum is going to happen very quickly."* Part of what is accelerating the timeline is AI itself. *"What is the true impact of AI in accelerating the development of future quantum computers, and then the extent to which quantum computers are used to develop AI?"* Mr. Mullally asked. AI helps identify where quantum can be applied, while quantum generates the kind of training data that AI cannot produce on its own.

Quantum advantage

Quantum advantage is a progression measured along two dimensions: scale (the number of error-corrected logical quantum bits, or qubits) and quality (the reduction of errors per operation). Today's quantum computers can run thousands of operations before errors overwhelm the result. The threshold for early commercial use cases—fraud detection, anomaly detection, complex pattern recognition—is millions of operations. *"Once we cross into millions of quantum operations, that's advantage,"* said Mr. Mullally. At billions of operations, current encryption standards begin to break—a watershed predicted to arrive in the early 2030s.

- **Regulatory frameworks for stablecoins no longer treat them as a background technology.** The GENIUS Act opens up a payment infrastructure that was previously accessible only to banks. *"All of a sudden you have this digital instrument where you do not need a bank to settle and clear payments,"* Ms. Massari told members. *"They are losing their payment monopoly."* Stablecoins allow organizations to move cash outside of operating hours, settle cross-border transactions in seconds, and execute AI-integrated payment flows that traditional banking infrastructure cannot support.
- **The talent questions looms.** *"Who is thinking about the talent pipeline development?"* one member asked. *"We already have a challenge with AI talent development."* New technologies require new kinds of expertise. Quantum computing demands mastery of both quantum physics and computer science, a rare combination of human training that takes years to develop. Audit committees should be asking management not only what the talent strategy is but also who is executing it and whether anyone within the organization has the requisite skill set.

Significant exposures sit outside the organization

In addition to the risks posed by the technologies themselves, audit committees must also contend with external risks: in the regulatory environment, in vendor and infrastructure dependencies, and in institutional partnerships that are available but underutilized.

Each of these external dimensions represents a category of risk that internal controls alone cannot address:

- **The regulatory situation is fluid.** The implementation of the GENIUS Act spans three federal banking agencies and state regulators, and the rules are still being finalized. Post-quantum

cryptography standards from the NIST and NSA are available, but adoption is currently voluntary, and most organizations have not incorporated them into vendor contracts or procurement requirements. On AI and cybersecurity, a new executive order[6] signed on June 2 contains both deregulatory provisions and requirements for government involvement in reviewing frontier AI models before release. *"With the latest executive order on AI, the government wants to strike the right balance,"* said Ms. Grimes. *"They want to be involved before some of these AI models come out to ensure their safety but also encourage innovation."*

- **Third-party and vendor activity presents hidden exposures.** Most organizations will address post-quantum cryptography exposure not directly but through their cloud providers and infrastructure vendors, which means their protection depends on those vendors' own quantum readiness. *"What is our plan with our third parties?"* Mr. Leatherman asked, describing the complexity of coordinating post-quantum cryptography transitions across supply chains. *"That is not an overnight thing. It is something we should be talking about now."* In cybersecurity, the perimeter has moved: the most common entry point for attackers is now edge infrastructure and third-party software vulnerabilities where third-party risk programs built for an earlier environment have not necessarily kept up.
- **Not all stablecoin issuers are the same.** Even with GENIUS regulation, the risks do not disappear. *"When you think about private keys and how those are managed and stored, there's operational risk there,"* said Mr. Maher. Evaluating issuers, understanding the infrastructure behind them, and establishing controls for how stablecoins are held and transacted are all things to start thinking about now.
- **The FBI can be a key partner for cybersecurity.** *"There are zero instances of an organization coming to the FBI and later saying, 'What was I thinking?'"* Mr. Leatherman said. *"There are many instances of organizations wishing they had engaged earlier. Days matter with this stuff—and with AI, even more."* The Cybersecurity Information Sharing Act of 2015[7] provides significant protection for information shared with the FBI: federal and state disclosure law exemptions, preservation of applicable privileges, and exemption from certain state and federal regulatory uses. *"If your lawyers aren't tracking this, they should be,"* Ms. Grimes said. *"Who manages the cyber risk? Is it the audit committee? Is it the technology committee? Is it the risk committee? Who has that ownership?"*

Looking ahead

The technologies discussed across these sessions present different timeframes for action, but what they share is a demand for preparation. *"Make sure you have the internal bandwidth to feel ready,"* said Mr. Phillips. Boards that have built habits of curiosity, external engagement, and honest risk assessments are better positioned to govern amid continuous technological change, not because they know more about quantum physics or blockchain architecture but because they ask the questions that reveal areas of risk that management may not have properly accounted for.

Reflection questions for audit committees

- ? Has management conducted a data audit that identifies the organization's most sensitive long-lived data, how it is encrypted, and what its lifespan of value is?
- ? Is post-quantum cryptography on the strategic risk register?
- ? Are the organizations you oversee defending against cyber threats at machine speed or still at human speed? What is management's plan to close that gap?
- ? Does your organization have a preexisting relationship with the FBI field office?
- ? Has the audit committee discussed stablecoins since the GENIUS Act? Does management have a view on whether the organization will interact with stablecoin payment infrastructure, and a framework for evaluating issuers if it does?
- ? Does management have the internal expertise to execute on the plans presented to the board across each of these three technology areas? How strong is the organization's capacity to absorb ongoing change?

About this document

The Audit Committee Leadership Network (ACLN) and Audit Committee Networks (ACNs) are groups of audit committee chairs drawn from leading North American and global companies committed to improving the performance of audit committees and enhancing trust in financial markets. The networks are 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.

Appendix 1: Participants

The following ACLN members participated in all or part of the meetings:

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

Tracey Travis, Accenture

Pat Yarrington, Lockheed Martin

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

Central Audit Committee Network

Candy Duncan, Teleflex

Mike Hanley, BorgWarner

Cary McMillan, Hyatt Hotels

Niharika Ramdev, Silgan

Derrick Roman, Vistance Networks and WEX

Phoebe Wood, Invesco and Legget & Platt

East Audit Committee Network

Brian Ford, Clearway Energy

Mary Choski, Omnicom Group

Maria Moats, Casey's General Stores

Leslie Seidman, Janus Henderson Group

Ruby Sharma, ATI, Inc.

Southeast Audit Committee Network

Joe Householder, Advanced Micro Devices

Jim Hunt, Brown & Brown

Mercedes Johnson, Synopsys and Teradyne

Maria Pinelli - Brightstar Lottery

Mimi Thigpen, Globe Life

Carol Yancey, BlueLinx

Bryan Yokley, Rayonier Advanced Materials

Southwest Audit Committee Network

Marcela Donadio, Norfolk Southern and NOV

Teri Fontenot, AMN Healthcare

Tom Gilligan, KB Homes

Sue Gove, LKQ Corporation

Don Kendall, Talos Energy

Cathy Lego, Guidewire Software

Hilliard Terry, Asbury Automotive

West Audit Committee Network-North

Phyllis Campbell, Remitly Global

Raman Chitkara, SiTime

Ken Goldman, Fortinet

Carol Hayles, eBay

Bala Iyer, Power Integrations

Meera Rao, Rambus

Janice Sears, Sonder Holdings

West Audit Committee Network-South

Michael Montelongo, Merlin

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

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

Lee Henderson, EY Americas Center for Board Matters Leader

Jennifer Lee, Managing Director, Americas Center for Board Matters

Molly Tucker McCue, EY US-East Assurance Managing Partner

Pat Niemann, Partner, Americas Center for Board Matters Leader

Juan Uro, EY Americas Strategic Relationships Office Leader

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

Dennis Andrade, Chief Executive

Kate Cady, Project and Event Manager

Jonathan Day, Vice Chair

Laura Koski, Project and Event Manager

Jo Rhoden, Executive Director

Ginevra Rollo, Senior Associate

Todd Schwartz, Executive Director

Ashley Vannoy, Project and Event Manager

Jason Watkins, Managing Director

Appendix 2: Guest biographies

Kristin Grimes is chief of the Cyber Law Unit within the National Security and Cyber Law Branch of the Federal Bureau of Investigation. Throughout her career, she has specialized in cyber issues, advising on data protection, incident response, supply chain security, and cyber regulatory compliance. Before joining the FBI, Ms. Grimes spent 16 years at a Fortune 500 cleared defense contractor, where she held roles including chief cyber counsel and intelligence analyst, and also served as an FBI assistant general counsel and as a Special Assistant United States Attorney in the Eastern District of Virginia. Prior to her legal career, she spent a decade working on operational and strategic counterintelligence, counterterrorism, and cyber issues for the U.S. intelligence community. Ms. Grimes holds a J.D. from the George Washington University Law School and M.A. and B.A. degrees from Seton Hall University, and is admitted to the Virginia bar.

Brett Leatherman is assistant director of the FBI's Cyber Division, where he leads the agency's strategy to impose cost on criminal and nation-state cyber actors consistent with the FBI's role as the lead US government cyber threat response agency. Prior to this role, he served as deputy assistant director for cyber operations, leading FBI teams responsible for high-impact domestic and global operations against cyber adversaries, and as executive director of the National Cyber Investigative Joint Task Force. As section chief of national security cyber operations, he partnered with the US Intelligence Community, foreign allies, and private sector leaders on a whole-of-government approach to state-sponsored cyber threats. Earlier in his career, Mr. Leatherman served in the FBI's Dallas Division as senior supervisory resident agent and assistant special agent in charge for national security, overseeing counterterrorism, counterintelligence, and cyber investigations across North Texas. Mr. Leatherman holds a degree in computer information systems from Cornerstone University and a master's degree in cybersecurity risk management from Georgetown University, and speaks internationally on emerging national security and cyber threats.

Brendan Maher is a Partner/Principal in EY's Financial Services Consulting practice, where he leads EY's digital assets product, operations, and risk solutions. He advises clients on product and operating model design, market structure changes, risk management, and regulatory change.

Jai Massari is of counsel at Arktouros PLLC, a boutique law firm, where her practice focuses on new forms of money and money networks. An executive and regulatory lawyer working at the intersection of financial services and technology, she is a lecturer at Stanford Law School, a trustee of the Practicing Law Institute, a member of the board of The Motley Fool, and an operating adviser at Bessemer Venture Partners. She was previously co-founder and chief legal officer of Lightspark and, before that, a partner in the financial institutions group of Davis Polk & Wardwell LLP in Washington, DC.

Gerald Mullally is chief executive officer at Oxford Quantum Circuits (OQC), where he leads the company's strategy and execution to scale quantum computing and deliver value for customers, partners, and shareholders. He has overseen OQC's expansion into global deployments, including systems in London, Tokyo, New York, and Spain, and the launch of the industry's first Quantum-AI Data Centre in collaboration with NVIDIA. He brings more than 20 years of experience delivering large-scale, mission-critical technology programs across financial services, energy, and defense, including roles at Accenture and PwC. Prior to OQC, he served for eight years in the UK government as a Director in the Prime

Minister's Office and Cabinet Office, where he led national security and resilience initiatives.

Simon Phillips is chief technology officer at Oxford Quantum Circuits (OQC), where he is responsible for the company's technology roadmap, development, and implementation to support commercialization. He leads efforts to scale OQC's engineering capabilities and translate its quantum computing technology into deployable commercial systems. He is an experienced technology executive and entrepreneur with a background in building and scaling technology businesses, including fundraising and international expansion. He has deep expertise in the quantum computing sector and in OQC's technical architecture and market positioning.

Steven Weber is a partner at Breakwater Strategy, where he focuses on strategy, decision-making, and scenario planning for complex challenges at the intersection of economics, technology, politics, regulation, and narrative. He is also a professor at the University of California, Berkeley, with a joint appointment in the School of Information and the Department of Political Science. Over a 30-year academic career, he has advised global firms, governments, and nonprofits on risk analysis, strategy, and communications, and is widely recognized for his work in scenario planning. Dr. Weber previously worked with Global Business Network and later with Monitor Group, helping organizations navigate technological and geopolitical transitions. He has also served as special political advisor to the first president of the European Bank for Reconstruction and Development. He is the founder of the Center for Long Term Cybersecurity at UC Berkeley and the author of *The Success of Open Source* and *Bloc by Bloc*.

Endnotes

[1] This document 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] Use of AI: Portions of this document may have been prepared with the assistance of AI tools. All content has been reviewed and approved by Tapestry Networks.

[3] Nellie Liang, "Stablecoins: Issues for Regulators as They Implement the GENIUS Act," *Brookings Institution,* October 21, 2025.

[4] Unit 42, "2026 Unit 42 Global Incident Response Report," Palo Alto Networks, February 17, 2026.

[5] "Operation Winter Shield," Federal Bureau of Investigation, accessed July 16, 2026.

[6] Exec. Order No. 14409, 91 Fed. Reg. 108 (June 2, 2026).

[7] Cybersecurity Information Sharing Act of 2015, 6 U.S.C. § 1501–1510.