Audit Committee Leadership Network

May 2022

ACLN

VIEWPOINTS

Government perspectives on sanctions and cybersecurity

World events over the last 12 months have heightened the cybersecurity and sanctions risks that large global companies face. Russia's invasion of Ukraine, an expanding list of sanctioned entities, and the intensifying threat of ransomware are creating new and complex challenges for companies, and new demands on their boards and audit committees.

On March 21-22, 2022, members of the Audit Committee Leadership Network (ACLN) met to hear perspectives of federal agencies that play lead roles on cybercrime, sanctions, and export controls. John Carlin, principal associate deputy attorney general with the United States Department of Justice (DOJ) and Jeff Sallet, a forensics and integrity services partner with EY who recently served as associate deputy director of the Federal Bureau of Investigation (FBI) joined the discussion. Mr. Carlin's comments were off the record; Mr. Sallet's comments were on the record.

For biographies of the guests, see Appendix 1 (page 8), and for a list of network members and other participants, see Appendix 2 (page 9).

Executive summary

Companies are confronting increased security challenges and risks due to sanctions, cyberattacks, and heightened geopolitical tensions. Members and guests discussed the increase in "blended cyber threats," in which nation states and criminal groups collaborate or a hostile nation encourages criminal attacks on its rivals. The conversation covered DOJ and FBI perspectives on sanctions and cybersecurity, along with important considerations for global public companies. Several major themes emerged from the discussion:[1]

- **Enforcement of sanctions and export controls is a top federal priority.** *(page 2)*

  The US government views sanctions and export controls as critical in responding to the invasion of Ukraine, and it is putting unprecedented levels of resources toward enforcement. Penalties may well be imposed for sanctions violations even where there is no criminal intent or even fault. Businesses are expected to conduct rigorous diligence, to establish comprehensive sanctions-compliance processes, to assign responsibility at the management level, and to define and document the board's oversight role.

tapestry NETWORKS

EY Building a better working world

- **Ransomware continues to be a major threat.** *(page 3)*

  Increased focus on sanctions and new cybersecurity disclosure proposals from the US Securities and Exchange Commission (SEC) create heightened compliance issues for public companies. Governance policies around ransomware should clearly delineate decision-making authority and processes. It is critical to check whether ransom payments could unknowingly go to a sanctioned entity. Working with the government—the FBI, DOJ, Department of Homeland Security, and/or Secret Service—can help a company's case if a payment is later deemed a violation of sanctions.

- **Proactively establishing a relationship with the FBI is essential.** *(page 5)*

  The FBI is committed to working with companies on cybersecurity and can provide significant assistance. The Bureau is keen to collaborate with the private sector, and companies should establish strong relationships with the FBI before any crisis occurs.

Enforcement of sanctions and export controls is a top federal priority

Members and guests discussed the Justice Department's approach to combatting corporate crime.[2] As geopolitical tensions continue to evolve, corporate crime can have significant national security implications. The Biden administration views sanctions and export controls as critical tools in responding to Russia's invasion of Ukraine, and the DOJ has stated that enforcement is a top priority.[3] The department is putting unprecedented levels of resources toward its enforcement efforts; overdeterrence is an explicit goal.

Members noted that sanctions are a "strict liability" regime, and penalties can be imposed even when a payment to a sanctioned entity is entirely unintentional. One member explained how sanctions apply not only to the entities themselves, but to organizations that own or control sanctioned entities, which adds increased complexity and risk: *"Even if you use, as many of us do, extensive databases to determine who your counterparties are in every transaction, in a place like Russia, you don't know if the third party you use is actually owned by a sanctioned entity."*

In this heightened enforcement environment, businesses must conduct rigorous diligence. Members and guests discussed several imperatives for global companies:

- **Establish clear oversight roles.** Accountability for compliance with sanctions and export controls should be clearly established, with oversight roles assigned at both management and board levels.

- **Ensure strong sanctions-compliance programs are in place.** While many companies have robust compliance programs for regulations such as anti-money laundering and the Foreign Corrupt Practices Act, their compliance programs for sanctions may not be as sophisticated. Boards and management should create and document policies and controls that include

sanctions compliance. They should also ensure that training is provided across the company, and potentially for supply chain partners.

- **Perform comprehensive sanctions screening.** Sanctions lists are expanding and scrutiny over compliance is increasing. Companies are expected to *"do everything they can to ensure sanctions are not violated,"* explained Mr. Sallet. One member commented on the growing complexity of sanctions risk and suggested that it would be helpful to know about new tools and resources to identify sanctioned entities. Another member said, *"No one knows who is on the sanctions list and who is not."* In addition to completing their own database checks, companies may need external help. Mr. Sallet noted that the major audit firms offer sanctions screening services and third-party risk evaluations.

Companies should prepare for a long-term focus on sanctions and export controls, which will likely include policy, enforcement, and litigation actions similar to those surrounding the Foreign Corrupt Practices Act today. In a post-session discussion, an ACLN member observed, *"This has implications not just with Russia, but for the allocation of capital in places that could be subject to significant sanctions in the future."* The DOJ continues to evolve its enforcement plans and has formed a new Corporate Crime Advisory Group[4] that will make assessments and propose recommendations for enforcement initiatives, including on sanctions and export controls.

Members also discussed the intersection of sanctions and ransomware. As companies face increasing threats from nation state actors—many of which are themselves sanctioned or tied to sanctioned entities—a ransom payment made to such groups could be considered a violation, whether or not the identity of the group was known at the time of payment.

Ransomware continues to be a major threat

Ransomware remains a top concern for companies. In addition to sanctions risk, proposed cybersecurity disclosure rules from the SEC create heightened compliance issues for companies facing ransomware attacks. The group explored the complex question of whether a company should pay a ransom and identified a range of good practices related to ransomware threats:

- **Establish clear governance policies regarding ransomware.** As a matter of policy, the FBI advises against paying ransom, arguing that doing so incentivizes future attacks. Nonetheless, members discussed scenarios in which companies may need to consider payment. For example, an attack could create life-threatening situations, jeopardize critical infrastructure, or put fiduciary responsibilities at risk. Boards and management should build policies and governance processes to support clear, rapid decision making. Policies should outline who can authorize a payment, what processes will be followed, and who will provide input into decisions (such as the general counsel, chief financial officer, and insurance

providers). Companies should also establish how the payment will be recorded, how the external auditor will be informed, and which government agencies will be notified.

- **Prioritize cyber resilience.** Companies should empower their cybersecurity teams for a heightened threat environment. *"Cyber resilience is key—have resilient backups, test your systems, and invest on the front end,"* said Mr. Sallet. He noted the importance of enforcing policies: *"Have consequences for people violating your cyber policies and procedures. There should be training, counseling, and then action because it is a huge risk area."*
- **Be extra vigilant to avoid paying sanctioned entities.** While paying a ransom may not in itself be illegal, paying a sanctioned entity is. If a company is contemplating a payment, it should ensure the perpetrator is not a sanctioned entity. Companies are encouraged to report ransomware attacks to the FBI, which can advise whether the identity of the attacker is known. In addition to internal sanctions screening, companies can seek input from other parties, such as third-party payment facilitators and insurance providers. If a payment is later deemed to violate sanctions, government agencies will view it favorably if the company can demonstrate that it pursued all avenues to identify the source of the attack and whether the entity receiving payment was sanctioned.
- **Revisit ransomware policies with an eye toward the SEC's proposed cybersecurity disclosure rules.**[5] Under these rules, a company would be required to disclose information about a cyber incident within four business days if it is determined to be material.[6] Determining materiality can be challenging, especially during the early stages of an attack. Companies should define who will be responsible for making the materiality determination and consider how this will be revisited throughout the incident. If materiality is unknown, companies can privately inform the SEC and keep enforcement officials updated as the incident progresses. Serious issues can arise if a ransomware payment is made but not disclosed. If a board determines that an attack is significant enough to warrant a payment but the company chooses to not make a disclosure, it could be difficult to later argue the attack was not material. By informing government agencies, a company may protect itself should an incident become worse.

ACLN members were interested in how to balance SEC disclosure requirements against the confidentiality requested by intelligence and law enforcement agencies. The FBI may ask a company to keep information private, at the same time that the SEC requires it to disclose material cybersecurity incidents. There are no easy solutions to this tension, but in a pre-meeting conversation, Mr. Sallet said: *"If the FBI asks you to keep information quiet, they can work with your general counsel and the DOJ to have that conversation with the SEC on the disclosure issues."*

Members and guests also discussed the connection between cryptocurrencies and ransomware attacks. Once widely believed to be almost impossible to trace, cryptocurrencies have been the payment method of choice for ransomware perpetrators. But the DOJ has

made strides in tracing cryptocurrency payments. In 2021, the FBI was able to recover $2.3 million of the Bitcoin ransom paid during the Colonial Pipeline attack.[7]

After the session, a member observed that *"one takeaway is to make sure we are revisiting policies: What is our ransom policy, our communications strategy, and how do we define materiality for disclosure?"*

Lessons from the FBI on insider threat

Corporate insiders pose significant threats, whether in the form of cyberattacks or acts such as espionage, sabotage, or theft. The frequency and costs of such incidents are increasing, especially cyber-related threats.[8] Yet many corporations do not have formal insider threat programs in place.[9]

Mr. Sallet oversaw insider threat as part of his responsibilities at the FBI, where espionage is a chief concern. He noted that it is increasingly important for companies to understand the risks posed by insiders and that boards and management can do more to mitigate the risk.

The process begins with hiring, Mr. Sallet said: *"Make sure you have good hiring policies and procedures in place and that you continue to monitor throughout careers."* Companies should thoroughly vet candidates before they are brought onboard. For ongoing monitoring, questions to consider include: Who has access to sensitive assets—both physical and virtual? How can you identify unusual patterns of behavior? How are you assessing environmental factors that could impact an employee's personal situation?

Boards should ensure that companies have strong detect-and-control policies and whistleblower systems. An executive committee or subcommittee focused on insider threat may be worth considering.

Proactively establishing a relationship with the FBI is essential

ACLN members and guests spoke about how companies can most effectively work with the FBI during a cyberattack. Several noted that corporations remain cautious about bringing law enforcement in during a cyber incident. They worried that disclosures flow only to the FBI and that information provided by the Bureau to companies may be outdated or lack value.

Mr. Sallet said that the FBI is committed to working closely with companies to provide aid during a cyberattack and to prevent and deter future attacks. Public-private collaboration is essential, he added: *"National security is a team sport, including the private sector, public*

sector, and government." One member observed that the government's approach to *"giving companies timely access to the threat stream has improved greatly."* Another said that *"there is more cooperation on the cyber front than there has been historically."*

The FBI can provide significant assistance, such as identifying an attacker or sharing insights about attack techniques. An ACLN member offered an example from a recent incident: *"One company I'm involved with had two ransomware attacks in the past 30 days. The FBI was tremendously useful to work with. They had a pretty good understanding of who was on the other end of the attack, and that really helped us."*

Mr. Sallet said that forming early relationships with the local FBI field office—before a crisis occurs—is an essential step. *"If you're exchanging business cards during a crisis, you have failed,"* he said. He advised members: *"As audit committee chairs, you should ask your company: Do they have an established relationship with the FBI? Do they have a relationship with the Department of Homeland Security?"* FBI field offices are now assessed on relationships with corporations in their area, Mr. Sallet noted, underscoring the importance the agency places on collaboration. In a debrief session, a member observed that *"the fact that there is an incentive for field offices to build relationships with corporate entities in their jurisdiction is good and companies should take advantage of that."*

Mr. Sallet also pointed out that the FBI can grant clearances to corporate leaders, which can lessen challenges around classified information and enhance information sharing.

About this document

The Audit Committee Leadership Network is 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.

Appendix 1: Guest biographies

John P. Carlin is the principal associate deputy attorney general of the United States. In this role, he is a member of the Department of Justice's senior leadership and is the principal counselor to the deputy attorney general. Mr. Carlin assists in the leadership's oversight of all DOJ components, which include the 94 US attorney's offices, the National Security Division, the Criminal Division, and the DOJ's law enforcement bureaus. He previously served as the acting deputy attorney general.

Before joining the Office of the Deputy Attorney General, Mr. Carlin was in private practice as a partner at the law firm of Morrison & Foerster. He has held several other roles in the DOJ, including assistant attorney general for the National Security Division, responsible for protecting the country against international and domestic terrorism, espionage, cyber, and other national security threats. Mr. Carlin was also chief of staff and senior counsel to the director of the FBI, where he helped lead the Bureau's evolution to meet growing and changing national security threats, including cyber threats. A career federal prosecutor, Mr. Carlin was also the national coordinator of the DOJ's Computer Hacking and Intellectual Property Program and an assistant US attorney for the District of Columbia. He is the author of a book and other publications on domestic and international cyber threats.

Jeff Sallet is a Forensic & Integrity Services partner at Ernst & Young LLP (EY). He serves on the Investigations & Compliance team, with a primary focus on forensics services and investigations in the Northeast and Chicago.

Mr. Sallet has more than 25 years of experience in investigations, forensic accounting, government regulations, leadership, and communications. He previously served as associate deputy director of the FBI, third in command. As a special agent, Mr. Sallet incorporated forensic accounting with traditional methods to investigate terrorism and terrorism financing, fraud, corruption, and organized crime.

He is a certified public accountant in the Commonwealth of Massachusetts and a certified financial forensics professional. Mr. Sallet earned a BBA, with a focus in accounting, from the University of Massachusetts, Amherst, where he regularly speaks to students about career opportunities in accounting.

Appendix 2: Participants

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

- Eva Boratto, UPS
- Judy Bruner, Applied Materials and Seagate Technology
- Janet Clark, Texas Instruments
- Sam Di Piazza, AT&T
- Bill Easter, Delta Air Lines
- Lynn Elsenhans, Saudi Aramco
- Tom Freyman, AbbVie
- Fritz Henderson, Marriott
- David Herzog, MetLife & DXC Technology
- Charles Holley, Amgen
- Suzanne Nora Johnson, Pfizer
- Akhil Johri, Boeing and Cardinal Health
- Lori Lee, Emerson Electric
- Brad Martin, FedEx Corporation
- Leeny Oberg, Adobe
- Ann Marie Petach, Jones Lang LaSalle
- Paula Price, Accenture
- Kimberly Ross, Cigna
- Tom Schoewe, General Motors
- Leslie Seidman, General Electric Company
- Gerald Smith, Eaton Corporation
- Fred Terrell, Bank of New York Mellon
- Tracey Travis, Meta
- Jim Turley, Citigroup
- John Veihmeyer, Ford Motor Company
- Robin Washington, Salesforce
- David Weinberg, Coca-Cola Company

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

- Kelly Grier, US Chair and Managing Partner and Americas Managing Partner
- John King, EY Americas Vice Chair – Assurance
- Pat Niemann, Americas Leader, EY Audit Committee Forum

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] Lisa Monaco, "Deputy Attorney General Lisa O. Monaco Gives Keynote Address at ABA's 36th National Institute on White Collar Crime" (speech, Washington, DC, October 28, 2021).

[3] John Carlin, "John Carlin on Stepping up DOJ Corporate Enforcement" (speech, GIR Connect: New York, October 11, 2021).

[4] Monaco, "Deputy Attorney General Lisa O. Monaco Gives Keynote Address at ABA's 36th National Institute on White Collar Crime."

[5] US Securities and Exchange Commission, "SEC Proposed Rules on Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure by Public Companies," news release, March 9, 2022.

[6] US Securities and Exchange Commission, *Public Company Cybersecurity: Proposed Rules*, fact sheet, March 9, 2022.

[7] US Department of Justice, "Department of Justice Seizes $2.3 Million in Cryptocurrency Paid to the Ransomware Extortionists Darkside," news release, June 7, 2021.

[8] Cybersecurity and Infrastructure Security Agency, *Insider Threat Mitigation Guide* (Arlington: CISA, 2020), 2.

[9] Cybersecurity and Infrastructure Security Agency, *Insider Threat Mitigation Guide*, 4.