HINSHAW

Alerts

Key Takeaways from FinCyber Femmes Meeting on Navigating AI and Cybersecurity Laws

September 30, 2025
Privacy, Cyber & AI Decoded

Hinshaw partner Cathy Mulrow-Peattie recently participated in a panel discussion during the Q3 2025 FinCyber Femmes Meeting, hosted at IBM's office in New York City. The FinCyber Femmes bring together leading professionals in cybersecurity, financial services, and technology to discuss the rapidly evolving landscape of artificial intelligence (AI) and its intersection with cybersecurity laws and regulations.

Cathy and her panel explored the latest trends, challenges, and best practices for organizations seeking to employ AI while managing their cyber risk and regulatory compliance.

Here's a summary of key takeaways from this latest FinCyber Femmes panel:

- **According to IBM's Cost of Data Breach Report, 63 percent of organizations that experienced a data breach lacked AI governance.** This absence of oversight not only increased the cost and impact of cybersecurity incidents but also emphasized the criticality of cybersecurity controls with AI.
- **The panel discussed the growing sophistication of cyber threats, noting that one in six breaches involved attackers using AI tools (e.g., phishing, deepfakes), increasing the threat and attack landscape.** The panelists discussed how most AI attacks were made through SAAS platforms and/or supply chain providers, highlighting the importance of maintaining strong cybersecurity for third-party applications.
- **All panels at the conference emphasized that AI is here to stay and should be tested and used properly.** AI can help us make more informed decisions, enhance efficiency, and provide better and more customized services only if it is built and used responsibly.
- **The event discussions recommended that financial services organizations, and fintechs in particular, ensure they have AI and cybersecurity controls in place.** The panel referred the audience to existing controls set out in the Department of Financial Services Cybersecurity Regulation Part 500 and AI Guidance, GLBA Safeguard Rules requirements, and existing OCC model risk management practices to mitigate cybersecurity AI risk.

Attorneys

Cathy Mulrow-Peattie

Service Areas

Consumer Financial Services

Privacy, Security & Artificial Intelligence

- **The speakers also stressed the importance of implementing AI on a use-case basis, guided by an established governance structure and an organization's existing policies and procedures.** This approach helps set expectations for employees and prevents the risk of "shadow AI," the unauthorized or unmonitored use of AI tools within an organization.
- **Lastly, the audience was also reminded of two upcoming New York State Department of Financial Services (NYSDFS) Part 500 requirements going into effect on November 1, 2025, for covered entities.** These requirements include:

  (1) Having Multifactor Authentication in place for remote access to systems and applications; and

  (2) Implementing policies and procedures to develop and maintain documented assets and an accurate asset inventory of the covered entities' information systems. Information systems are broadly defined and cover any system that collects, processes, stores, uses, shares, or discloses electronic information.