

### Agenda

- 3:30 – 4:00 PM **In-person Registration**  
*Light refreshments available for those on-site*
- 3:50 PM **Virtual guests log on**
- 4:00 PM **Welcome**
- 4:00 – 5:00 PM
1. **Overview: a history of cyber security breaches**
    - In the news: recent breaches
    - What's changing and in terms of techniques and vulnerabilities
  2. **You've been hacked, now what?**
    - What are the main considerations from an in-house perspective?
      - Internal incident response and remediation
      - Third party engagement (law firm, forensic firm)
      - Breach notification (individuals, suppliers, etc.)
      - Regulatory notification / engagement
      - Law enforcement engagement
      - Media Relations
      - Insurance
      - Litigation
    - Outside Counsel perspective
      - Maintaining privilege in light of Capital One, Clark Hill and Rutters
      - Who hires? Who supervises?
      - Controlling the messaging
    - Law enforcement/FBI perspective
      - What is the FBI doing?
      - What does the FBI want companies to do?
      - What are the realities?
      - Can I get my money back?
  3. **Regulatory and legislative updates**
    - Enforcement Actions
    - New passed/proposed rules
      - SEC
      - NYDFS
      - NIST cybersecurity framework 2.0
  4. **Conclusion**

Moderator:

- Celia Cohen, Ballard Spahr LLP

Panelists:

- Douglas Bloom, Managing Director, Co-Head of Cybersecurity and Privacy Law, Morgan Stanley
- Mia C. Korot, Executive Director, Assistant General Counsel, Cybersecurity & Global Security, JPMorgan Chase & Co
- William R. McKeen, Supervisory Special Agent- Cyber Division, Federal Bureau of Investigation
- Phil Yannella, Ballard Spahr LLP

- 5:00 – 6:00 PM **Networking Reception**