



— **CLE Credits:**

This program is approved for 1.0 CLE credit in CA, NV, NY (Cybersecurity – General), & PA; and 1.2 NJ.

Uniform Certificates of Attendance will also be provided for the purpose of seeking credit in other jurisdictions





For our guests attending in person:

- Please complete the CLE Evaluation Form that was provided to you at registration
- Ensure you have signed in for CLE credit

For guests participating virtually:

- There will be poll questions throughout the afternoon.
- Be sure to answer all the polls you see for the duration you are logged in to receive the appropriate amount of CLE credits

Panelists

			
Douglas Bloom Morgan Stanley	Mia Korot JPMorgan Chase & Co.	Will McKeen Federal Bureau of Investigation	Phil Yannella Ballard Spahr LLP



Overview

Ballard Spahr LLP

— A history of cyber security breaches

- Examples of recent breaches
- What's changing and in terms of techniques and vulnerabilities



— What's In a Number?

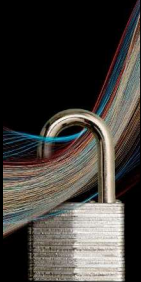
2023 Reported Victims in NYC

16,771



— What's In a Number?

2023 Total Reported Losses in NYC
630,000,000



— What's In a Number?

2023 Total Reported Losses in US
4,600,000,000



Recent Significant Cases



A New Kind of Third Party Risk



Defeating MFA The Old-Fashioned Way



AI Trade Secret Theft



Common Tactics, Techniques, Procedures





— Regulatory Update: Securities & Exchange Commission

- Final SEC rule on Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure was published in the Federal Register on August 4, 2023
- These are the new disclosure requirements for publicly traded companies and, in certain instances, foreign private issuers
 - December 18, 2023: All companies other than smaller reporting companies must report material cybersecurity incidents on Form 8-K and Form 6-K
 - June 15, 2023: Date for smaller companies
 - All issuers will be required to tag Form 8-K and Form 6-K disclosures beginning December 18, 2024
 - New disclosures in Annual Reports on Form 10-K and Form 20-F will be required in reports for FYs ending on or after December 15, 2023



— Regulatory Update: New York Department of Financial Services

- On November 1, 2023, NYDFS finalized the amendment to its cybersecurity regulation
 - (1) new requirements for larger, companies (so-called “Class A Companies”)
 - (2) expanded governance requirements for boards, senior officers, and chief information security officers (as defined below)
 - (3) expanded cyber incident notice and compliance certification requirements
 - (4) new requirements for incident response and business continuity planning; and
 - (5) an expanded multi-factor authentication requirement for user access to a company’s network.



— Regulatory Update: Federal Trade Commission

- On October 27, 2023, the FTC amended the Safeguards Rule
- Requires non-banking financial institutions, such as mortgage brokers, motor vehicle dealers, and payday lenders, to report data breaches and security events to the FTC
- Will become effective 180 days after publication in the Federal Register
- Financial institutions subject to the authority of the FTC will be required to notify the Agency as soon as possible, and no later than 30 days after discovery of a “Notification Event” impacting 500 or more consumers



— Legislative Update: National Institute of Standards and Technology (NIST)

- February 12, 2014: NIST issued the Framework for Improving Critical Infrastructure Cybersecurity (CSF)
- April 16, 2018: NIST issued the CSF 1.1, which included updates on supply chain risk management, vulnerability disclosure, among other issues
- August 8, 2023: NIST published a draft of the CFS 2.0
 - expands the use of the CSF
 - more fully embraces supply chain risk management
 - updates other frameworks and resources,
 - supplies implementation guidance, addresses cybersecurity measurement and assessment
 - adds an entirely new function (Govern), which covers how organizations make and execute decisions around cybersecurity; this is in addition to the other five functions are Identify, Protect, Detect, Respond, and Recover



— In-House Counsel Perspective

- Internal incident response and remediation
 - Secure operations – fix vulnerabilities and mobilize response team
 - Investigate
 - Stop additional data loss
 - Fix vulnerabilities
- Third party engagement
 - law firm
 - forensic firm



— In-House Counsel Perspective

- Breach notification
 - Individuals
 - Third party suppliers
 - Regulatory notification / engagement
 - Law enforcement engagement
 - Media Relations
 - Did the breach involve electronic personal health records? (check FTC and HHS rules)
- Insurance
- Litigation



— Outside Counsel Perspective

- **Litigation Risks:** Rise in Business to Business Litigation and how to mitigate risks
- **Who hires? Who supervises?**
- **Maintaining privilege:** Breach reports must include legal opinions or tactics, or be for the purpose of litigation to be protected. Reports done by consultants that are for business continuity likely will not be protected.
 - *In re Capital One Consumer Data Security Breach Litigation*
 - *Wengui v. Clark Hill*
 - *In re Rutter's Data Security Breach Litigation*
- **Controlling the messaging**



— Outside Counsel Perspective

- **Enforcement Risks**
 - The SEC charged Software Company Blackbaud Inc. for Misleading Disclosures about Ransomware Attack that Impacted more than 13,000 customers (March 9, 2023)
 - The SEC charged SolarWinds and its chief information security officer for fraud and intentional control failures relating to allegedly known cybersecurity risks and vulnerabilities (October 30, 2023)



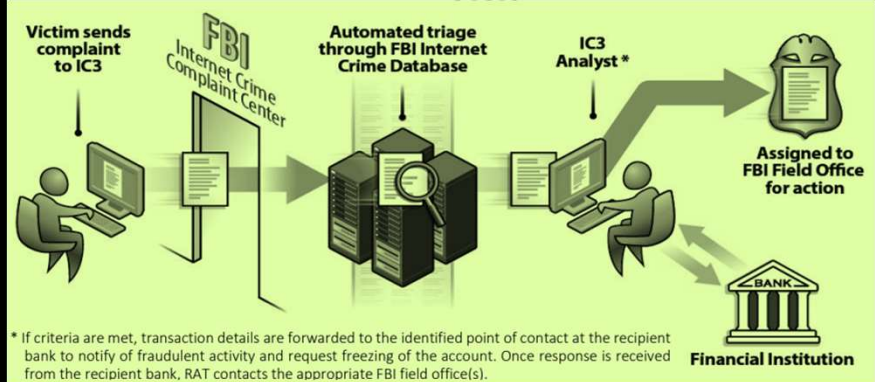
Law Enforcement/FBI Perspective

- What is the FBI doing?
- What does the FBI want companies to do?
- What are the realities?
- Can I get my money back?



Involving Law Enforcement

Goal #1: Get Your Money Back



CYBER

