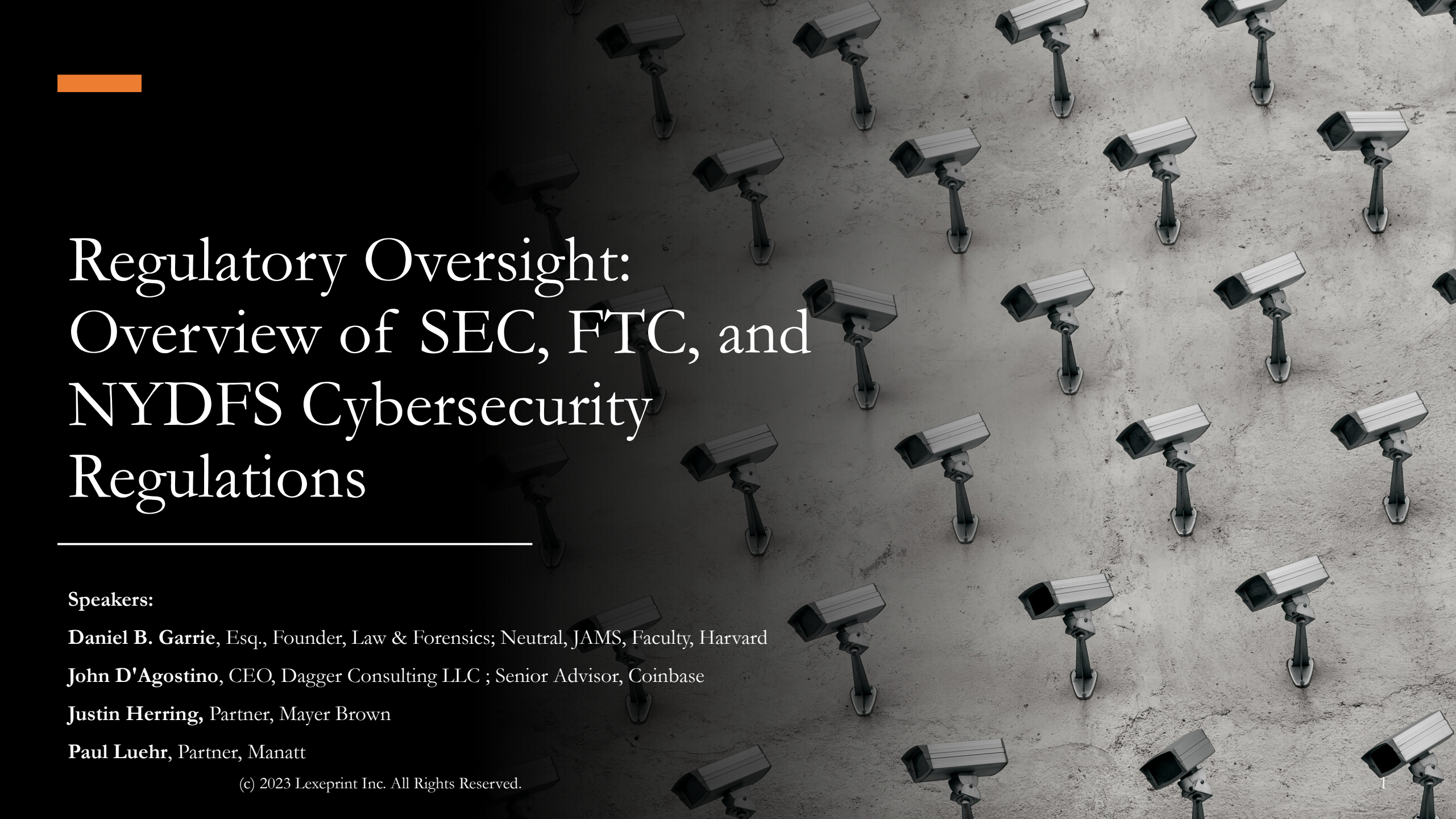


# Regulatory Oversight: Overview of SEC, FTC, and NYDFS Cybersecurity Regulations


**Speakers:**

**Daniel B. Garrie**, Esq., Founder, Law & Forensics; Neutral, JAMS, Faculty, Harvard

**John D'Agostino**, CEO, Dagger Consulting LLC ; Senior Advisor, Coinbase

**Justin Herring,** Partner, Mayer Brown

**Paul Luehr**, Partner, Manatt


(c) 2023 Lexeprint Inc. All Rights Reserved.

# Disclaimer



This is not legal advice, nor should it be considered legal advice.



The participants' comments today represent only their personal views, and do not reflect those of their employers or clients.



This presentation is offered for educational and informational uses only. These slides have been prepared for purposes of generating a discussion with our participants.



Soliciting speakers is strictly prohibited.

(c) 2023 Lexeprint Inc. All Rights Reserved.

# Speakers



**Daniel B. Garrie, Esq.**
Founder, Law & Forensics
Neutral, JAMS
Faculty, Harvard



**John D'Agostino**
CEO,
Dagger Consulting LLC;
Senior Advisor, Coinbase



**Justin Herring**
Partner,
Mayer Brown



**Paul Luehr**
Partner, Manatt

(c) 2023 Lexeprint Inc. All Rights Reserved.

# Agenda

- SEC
  - Securities and Exchange Commission 2023 New Cybersecurity Rules
  - SEC Response to SolarWinds
- NYDFS
  - NYDFS Cybersecurity Regulation (23 NYCRR 500)
  - Proposed Changes to the NYDFS Cybersecurity Regulation
- FTC
  - FTC Cybersecurity Enforcement Capabilities
  - Trade Regulation Rule on Commercial Surveillance and Data Security ANPR

(c) 2023 Lexeprint Inc. All Rights Reserved.

# What Regulatory Bodies Govern Public Corporations?

(c) 2023 Lexeprint Inc. All Rights Reserved

# Securities and Exchange Commission 2023 New Cybersecurity Rules

(c) 2023 Lexeprint Inc. All Rights Reserved.


This Photo by Unknown author is licensed under CC BY-NC.

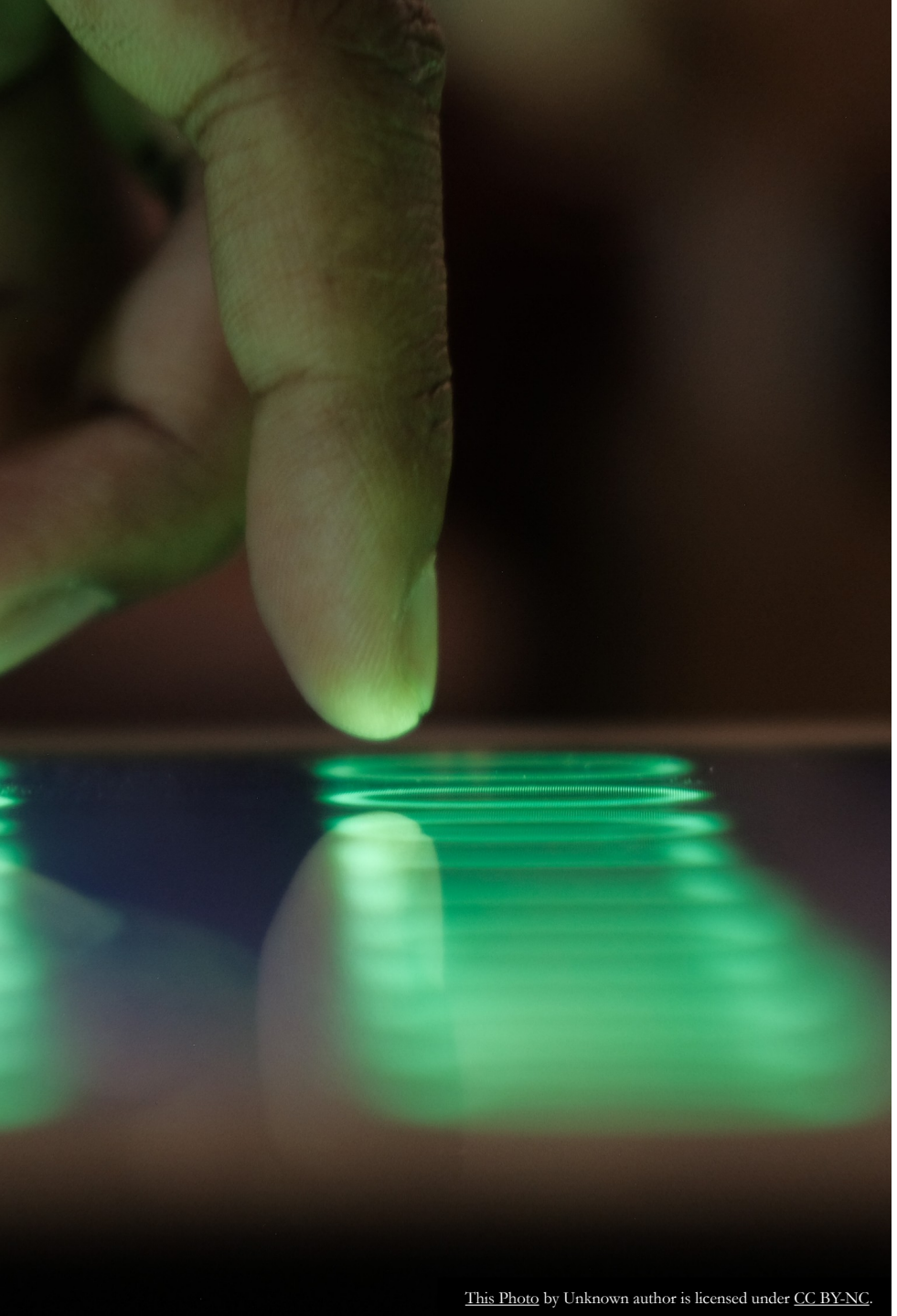
# SEC Adopts New Cybersecurity Rules

- In June 2023, the SEC adopted its "Rules on Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure by Public Companies."
- These new rules require registrants to disclose:
  - Material cybersecurity incidents,
  - Material information regarding their cyber risk, management, strategy, and governance.
- The final rules became effective in late July.

(c) 2023 Lexeprint Inc. All Rights Reserved.

# Why Are Regulators Looking for Increased Transparency From Corporations?

(c) 2023 Lexeprint Inc. All Rights Reserved


This Photo by Unknown author is licensed under CC BY-NC.

# Role and Motivation for the New Rule

"Currently, many public companies provide cybersecurity disclosure to investors. I think companies and investors alike, however, would benefit if this disclosure were made in a more consistent, comparable, and decision-useful way. Through helping to ensure that companies disclose material cybersecurity information, today's rules will benefit investors, companies, and the markets connecting them."

**SEC Chair Gary Gensler*

(c) 2023 Lexeprint Inc. All Rights Reserved.



This Photo by Unknown author is licensed under CC BY-NC.

# Timely Disclosure of Incidents

- Companies must disclose "any cybersecurity incident they determine to be material' on new Item 1.05 of Form 8-K.
- The disclosures must describe materials aspects of the incident, including:
  - Nature
  - Scope
  - Timing
  - Material impact
  - Reasonably likely material impact
- Item 1.05 of Form 8-K will be due 4 business days "after a registrant determines that a cybersecurity incident is material."
  - Disclosure delays will be determined by the USAG

(c) 2023 Lexeprint Inc. All Rights Reserved.


This Photo by Unknown author is licensed under CC BY-NC.

# Detailed Reporting on Cybersecurity Management

- The rules added Regulation S-K Item 106, which requires companies to describe:
  - Processes for assessing, identifying, and managing material risks.
  - Material effects or reasonably likely effects of risk from:
    - Cybersecurity threats, and
    - Previous cybersecurity incidents.
  - "The board of directors' oversight of risk from cybersecurity threats."
  - "Management's role and expertise in assessing and managing material risk from cybersecurity threats."
- The disclosures will be required in registrants' annual report on Form 10-K.

**SEC, Public Company Cybersecurity Disclosures; Final Rules*

(c) 2023 Lexeprint Inc. All Rights Reserved.


This Photo by Unknown author is licensed under CC BY-NC.

# Regulation S-K Item 106: Board Requirement

- The disclosure of the board's role identified in Item 106(c)(1) requires registrants to:
  - Describe the board's oversight of risk from cybersecurity threats.
  - Identify board committees or sub-committees responsible for cybersecurity risk oversight.
  - Describe the process by which the board is informed of risk from cyber threats.
- This requirement is narrower than the proposed rules, which would have required information about "how cybersecurity related to the registrant's business strategy" and the frequency of cybersecurity discussions at board meetings.

**SEC, Public Company Cybersecurity Disclosures; Final Rules*

(c) 2023 Lexeprint Inc. All Rights Reserved.


This Photo by Unknown author is licensed under CC BY-NC.

# Regulation S-K Item 106: Management's Role

- Item 106(c)(2) directs registrants to "consider disclosing":
  - "Whether and which management positions or committees are responsible for assessing and managing such risks, and the relevant expertise of such persons or members in such detail as necessary to fully describe the nature of the expertise;
  - The processes by which such persons or committees are informed about and monitor the prevention, detection, mitigation, and remediation of cybersecurity incidents; and
  - Whether such persons or committees report information about such risks to the board of directors or a committee or subcommittee of the board of directors."

*SEC, Public Company Cybersecurity Disclosures; Final Rules*

(c) 2023 Lexeprint Inc. All Rights Reserved.


This Photo by Unknown author is licensed under CC BY-NC.

# Foreign Private Issuers

- Foreign private issuers have comparable requirements to covered domestic companies:
  - Form 6-K for material cybersecurity incidents
  - Form 20-F for cybersecurity risk management, strategy, and governance.

**SEC, Public Company Cybersecurity Disclosures; Final Rules*

(c) 2023 Lexeprint Inc. All Rights Reserved.



This Photo by Unknown author is licensed under CC BY-NC.

# Disclosure Due Dates

- "The Form 10-K and Form 20-F disclosures will be due beginning with annual reports for fiscal years ending on or after December 15, 2023."
- "The Form 8-K and Form 6-K disclosures will be due beginning the later of 90 days after the date of publication in the Federal Register or December 18, 2023."
- "Smaller reporting companies will have an additional 180 days before they must begin providing the Form 8-K disclosure."

**SEC, Public Company Cybersecurity Disclosures; Final Rules*

(c) 2023 Lexeprint Inc. All Rights Reserved.

# What are Some of the Potential Risks and Challenges of Increased Disclosures?

(c) 2023 Lexeprint Inc. All Rights Reserved


This Photo by Unknown author is licensed under CC BY-NC.

# Potential Security Risk from Disclosure Requirements

- The new SEC rules seek to increase transparency and accountability through the disclosure of cyber incidents and risk management practices.
  - Yet the very descriptions of processes necessary to comply with these new rules have the potential to further threaten the security of organizations.
- These disclosure may give malicious actors insights into how organizations protect themselves, potentially helping them to identify blind spots or weaknesses to be targeted.

(c) 2023 Lexeprint Inc. All Rights Reserved.


This Photo by Unknown author is licensed under CC BY-NC.

# Trade Secret Considerations

- The disclosures required may also present a threat to the protection of corporations' trade secrets that are based on technical or engineering know-how of cyber risk management, as they may help reveal:
  - Plans, methods, techniques, processes, procedures, and programs.
- This access may in turn enable threat actors to subvert the remediation measures disclosed, enabling continued access and undermining their intent.

(c) 2023 Lexeprint Inc. All Rights Reserved.


This Photo by Unknown author is licensed under CC BY-NC.

# Balancing Compliance with Trade Secret Protection

- The trade secret protection challenges that these new rules engender will require business to balance:
  - Transparency and compliance with the required disclosures, and
  - Protecting the know-how against cyber threats and investor interests.
- Disclosures may additionally undermine shareholder and customer trust, potentially diminishing the perceived value of trade secrets.
  - This outcome may support the SEC's intention to increase accountability for regulated companies, but to the detriment of those most transparent in their disclosures.

(c) 2023 Lexeprint Inc. All Rights Reserved.



# SEC Response to SolarWinds Data Breach

(c) 2023 Lexeprint Inc. All Rights Reserved.

# What is the Role of Regulators Following Cyber Attacks? How Can They Shape Corporate Behavior?

(c) 2023 Lexeprint Inc. All Rights Reserved



This Photo by Unknown author is licensed under CC BY-SA-NC

# SEC Response to Solar Winds

- Following disclosure of the breach:
  - SolarWinds told the SEC that up to 18,000 of its customers installed updates that left them vulnerable to hackers.
- The US Securities and Exchange Commission (SEC) then:
  - Investigated companies that failed to disclose the effects of the SolarWinds hack.
  - Offered amnesty to companies that came forward and disclose the impact of the hack on their business.
  - Stated it would pursue enforcement actions and heightened penalties for companies that had not properly disclosed the impact of the hack.

(c) 2023 Lexeprint Inc. All Rights Reserved.



# Wells Notice

- SolarWinds, which is publicly traded, has faced a number of shareholder derivative lawsuits since the lawsuit, some of which have been settled and others dismissed.
- In June 2023, the SEC notified current and former SolarWinds executives, including the CISO and CFO, that it is planning on bringing enforcement action against them through a Wells Notice relating to the 2020 breach.
- The SEC previously expressed concern with the company's disclosures and public statements, as well as procedures leading up to and after the breach.
- In response, SolarWinds spokespersons and executives have emphasized their cooperation efforts with regulators.

(c) 2023 Lexeprint Inc. All Rights Reserved.



# Significance of the Wells Notice

- This Wells Notice is notable as it is likely the first time a CISO is directly named in such a notice.
- This action reflects the increasing regulatory and judicial scrutiny over businesses' cyber risk management practices and the individual responsibility of key executives, specifically that of CISOs.
- The trend is further emphasized in the recent *U.S. v. Joseph Sullivan* case, which demonstrates that CISOs are not immune from facing criminal charges for their actions.

(c) 2023 Lexeprint Inc. All Rights Reserved.



This Photo by Unknown author is licensed under CC BY-SA.

# NYDFS Cybersecurity Regulation (23 NYCRR 500)

## 23 NYCRR 500

This Photo by Unknown author is licensed under CC BY-SA.

(c) 2023 Lexeprint Inc. All Rights Reserved.



This Photo by Unknown author is licensed under CC BY-SA

# What is the NYDFS?

- In October 2011, the New York State Insurance Department and New York State Banking Department were consolidated to create the New York State Department of Financial Services (NYDFS)
- The New York State Department of Financial Services (NYDFS) is responsible for reforming and regulating financial services and products in the state of New York

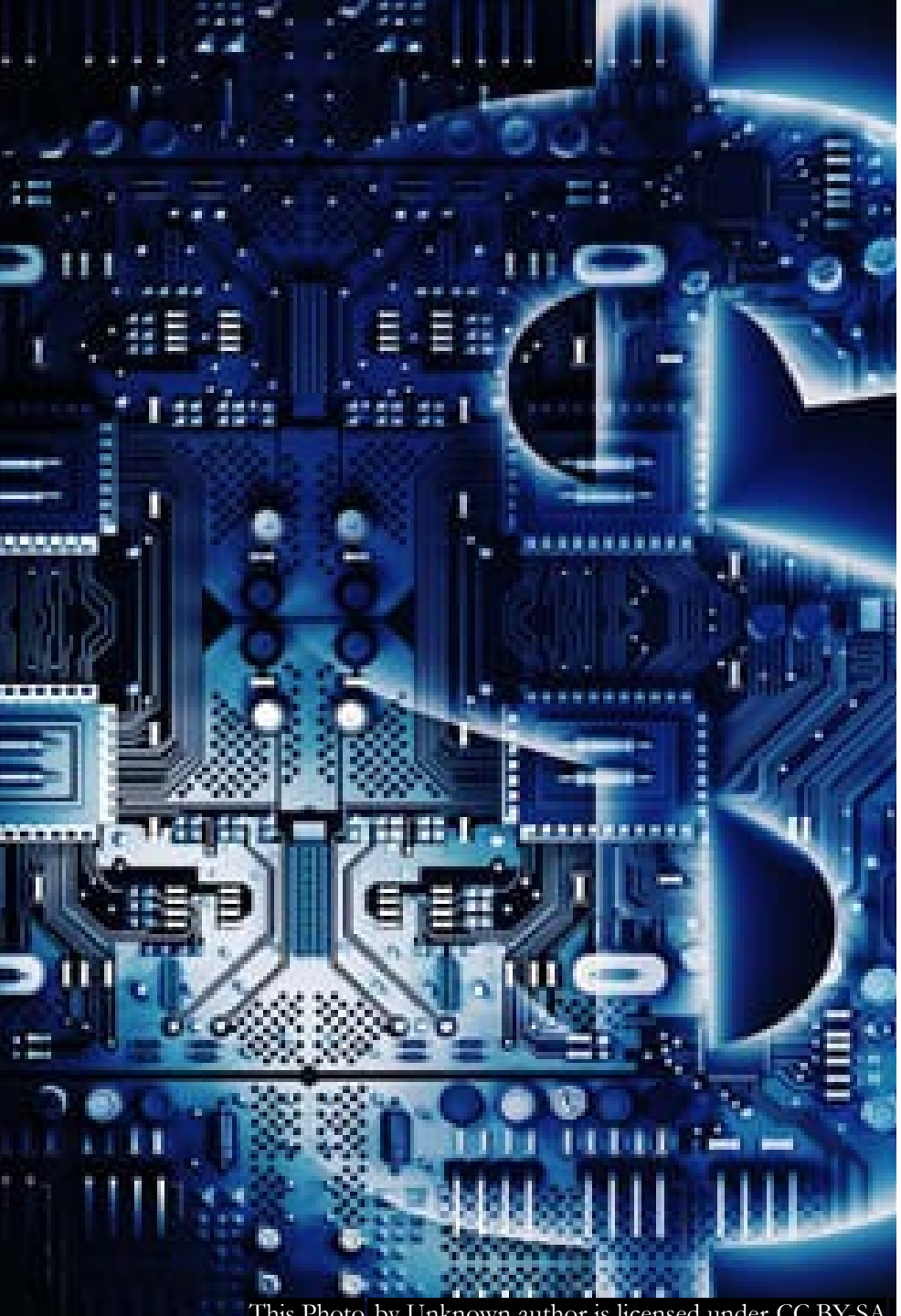
(c) 2023 Lexeprint Inc. All Rights Reserved.



# What is the NYDFS?

- According to the NYDFS Mission, the Superintendent may take any legal actions necessary to:
  - Foster the growth of the financial industry in New York,
  - Ensure the continued solvency and safety financial service providers,
  - Ensure fair, timely and equitable fulfillment of the financial obligations,
  - Protect users of financial products and services,
  - Encourage high standards of honesty, transparency, fair business practices and public responsibility,
  - Eliminate criminal abuse and unethical conduct in the industry, and
  - Educate and protect users of financial products and services.

(c) 2023 Lexeprint Inc. All Rights Reserved.


This Photo by Unknown author is licensed under CC BY-SA

# What is the NYDFS Cyber Security Regulation (23 NYCRR 500)?

- On March 1, 2017, NYS introduced 23 NYCRR 500, a regulation that demands financial companies implement a detailed framework to better protect consumer data privacy
- The 23 NYCRR 500 is part 500 of the NYDFS's overall body of regulation and requires supervised entities to assess their cybersecurity risk profiles and implement a comprehensive plan that recognizes and mitigates that risk.
- Six regulatory minimum standards have been set to assist organizations in preventing data breaches.

(c) 2023 Lexeprint Inc. All Rights Reserved.

# What Are Some of the Challenges of Balancing Consumer Privacy with Business Priorities?

(c) 2023 Lexeprint Inc. All Rights Reserved




# 1. Maintain a Program

Each covered entity must maintain a cybersecurity program designed to protect the confidentiality and integrity of the entity's information systems. This program should perform the following functions:

- Identify and assess cybersecurity risks that threaten stored nonpublic information;
- Detect cybersecurity events and respond to such events; and
- Mitigate and recover from such events using defensive infrastructure and implemented policies and procedures. *

** 23 NYCRR 500.2*

(c) 2023 Lexeprint Inc. All Rights Reserved.



# 2. Qualified CISO

- The regulation requires that a program is overseen by a chief information security officer (CISO) and implemented by qualified cybersecurity personnel.
- The CISO is responsible for creating a report in writing to the company's governing body on the company's cybersecurity program, including:
    - The confidentiality of NPI;
    - The entity's cybersecurity policies and procedures;
    - Material cybersecurity risks to the entity;
    - The overall effectiveness of its cybersecurity program; and
    - Material cybersecurity events involving.

(c) 2023 Lexeprint Inc. All Rights Reserved.

** 23 NYCRR 500.2*



This Photo by Unknown author is licensed under CC BY-SA

# 3. Effective Incident Response Plan

- The cybersecurity program must include an effective incident response plans to respond to and recover from any cybersecurity event. The incident response plan should address the following areas:
  - The goals of the incident response plan;
  - The internal processes and responsibilities of decision-making authority for responding to a cybersecurity event;
  - Identification of requirements for the remediation of any identified weaknesses;
  - Documentation and reporting regarding cybersecurity events; and
  - The evaluation of the incident response plan following a cybersecurity event.*

**Source: 23 NYCRR 500.16 & 500.2*

(c) 2023 Lexeprint Inc. All Rights Reserved.



# 4. Procedures and Controls

- Each entity covered by the regulation must implement risk-based procedures and controls designed to monitor the activity of authorized users and detect unauthorized access or use of nonpublic information by such authorized users.
- As such, it is required that such entities provide regular cybersecurity awareness training for all personnel. *

*Source: 23 NYCRR 500.14

(c) 2023 Lexeprint Inc. All Rights Reserved.



# 5. Systems and Risk Assessment

- All covered entities need to maintain systems that, based on its risk assessment:
  - Are designed to sufficiently reconstruct material financial transactions to support its normal operations; and
  - Include audit trails designed to detect and respond to cybersecurity events that have a reasonable likelihood of materially harming the entity's normal operations.

*Source: 23 NYCRR 500.6

(c) 2023 Lexeprint Inc. All Rights Reserved.



# 6. Periodic Review of Program

- A company must provide periodic risk assessments of its information systems to inform the design of their cybersecurity program.
- The risk assessment should be updated "as reasonably necessary to address changes" to technological developments and evolving threats.

*Source: *23 NYCRR 500.9*

(c) 2023 Lexeprint Inc. All Rights Reserved.



# 6. Periodic Review of Program (cont.)

- The risk assessment should be carried out in accordance with written policies and procedures, including:
  - (1) criteria for the evaluation and categorization of identified cybersecurity risks;
  - (2) criteria for the assessment of the confidentiality, integrity, security and availability of the covered entity's information systems and nonpublic information; and
  - (3) requirements describing how identified risks will be mitigated or accepted.*

*Source: *23 NYCRR 500.9*

(c) 2023 Lexeprint Inc. All Rights Reserved.

# What Are Some of the Basic Safeguards Businesses Can Implement Against Cyber Threats?

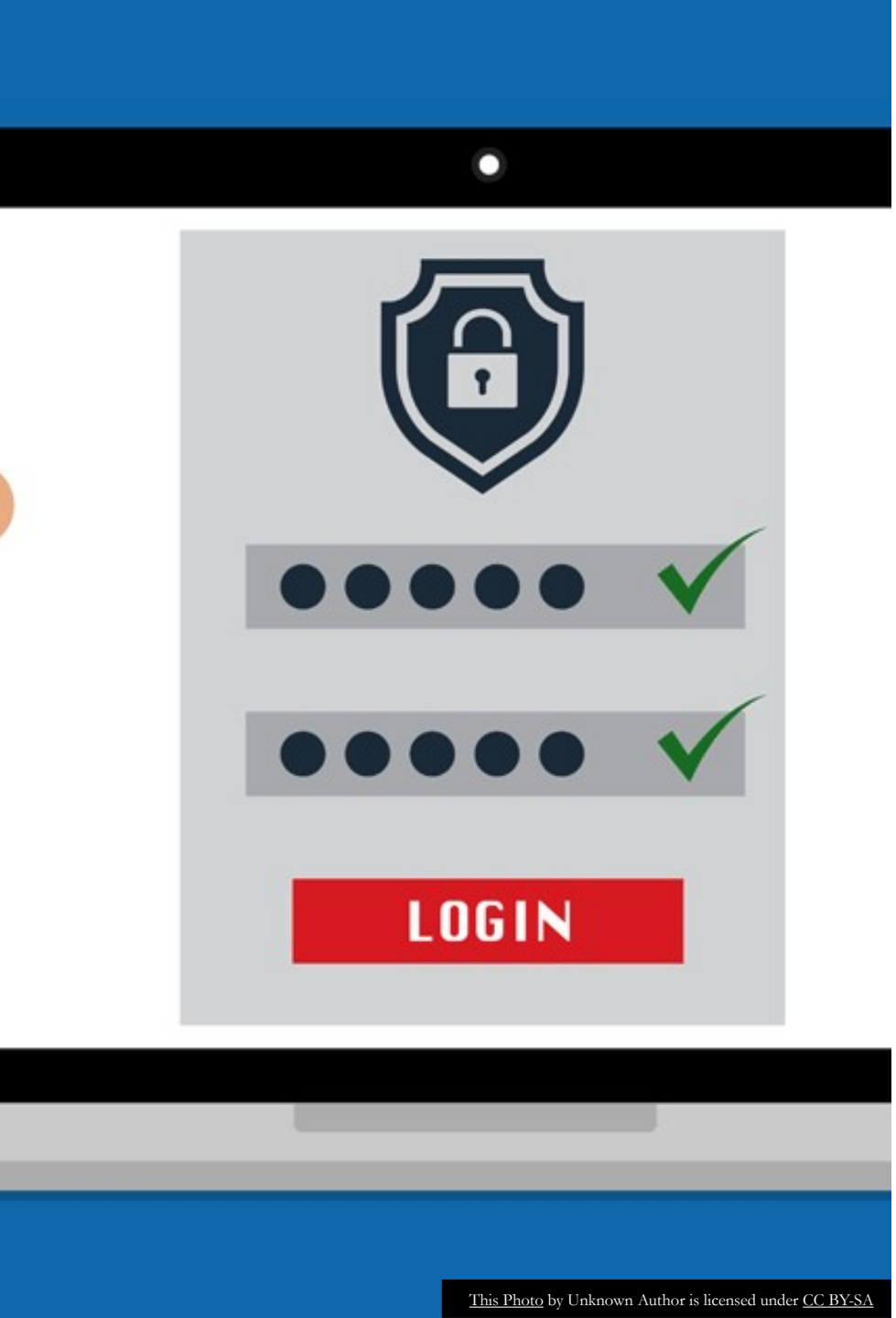
(c) 2023 Lexeprint Inc. All Rights Reserved



# Technical Control: Multi-Factor Authentication

- Multi-Factor Authentication (MFA) is an authentication system that requires more than one distinct authentication factor for successful authentication.
- MFA is one of the few technical controls explicitly required by 23 NYCRR Part 500 and remains increasingly essential because of the growing risk of cybercrime.
- MFA weaknesses are the most common cybersecurity gap exploited at financial services companies, according to the DFS, which found that more than 18.3 million consumers were impacted in a calendar year by cyber incidents reported to DFS pursuant to Section 500.17(a) in which Covered Entities had MFA failures.
    - According to Microsoft, MFA blocks 99.9% of automated cyber-attacks.

(c) 2023 Lexeprint Inc. All Rights Reserved.




This Photo by Unknown Author is licensed under CC BY-SA

# Guidance on Multi-Factor Authentication (cont'd)

- As a result, DFS focuses on the implementation of its regulation's MFA requirements and outlines common problems related to MFA and recommendations of courses of action.
- DFS details the most common reasons for violations of the Section 500.12 requirement for MFA.
  - **(1) Legacy Systems That Do Not Support MFA:** Covered Entities who use outmoded applications and systems, "legacy systems," that do not support MFA.
  - (2) **MFA for Remote Access Fails to Cover Key Applications:** many Covered Entities have email or other applications that can be accessed without VPN access.

(c) 2023 Lexeprint Inc. All Rights Reserved.




# Guidance on Multi-Factor Authentication (cont'd)

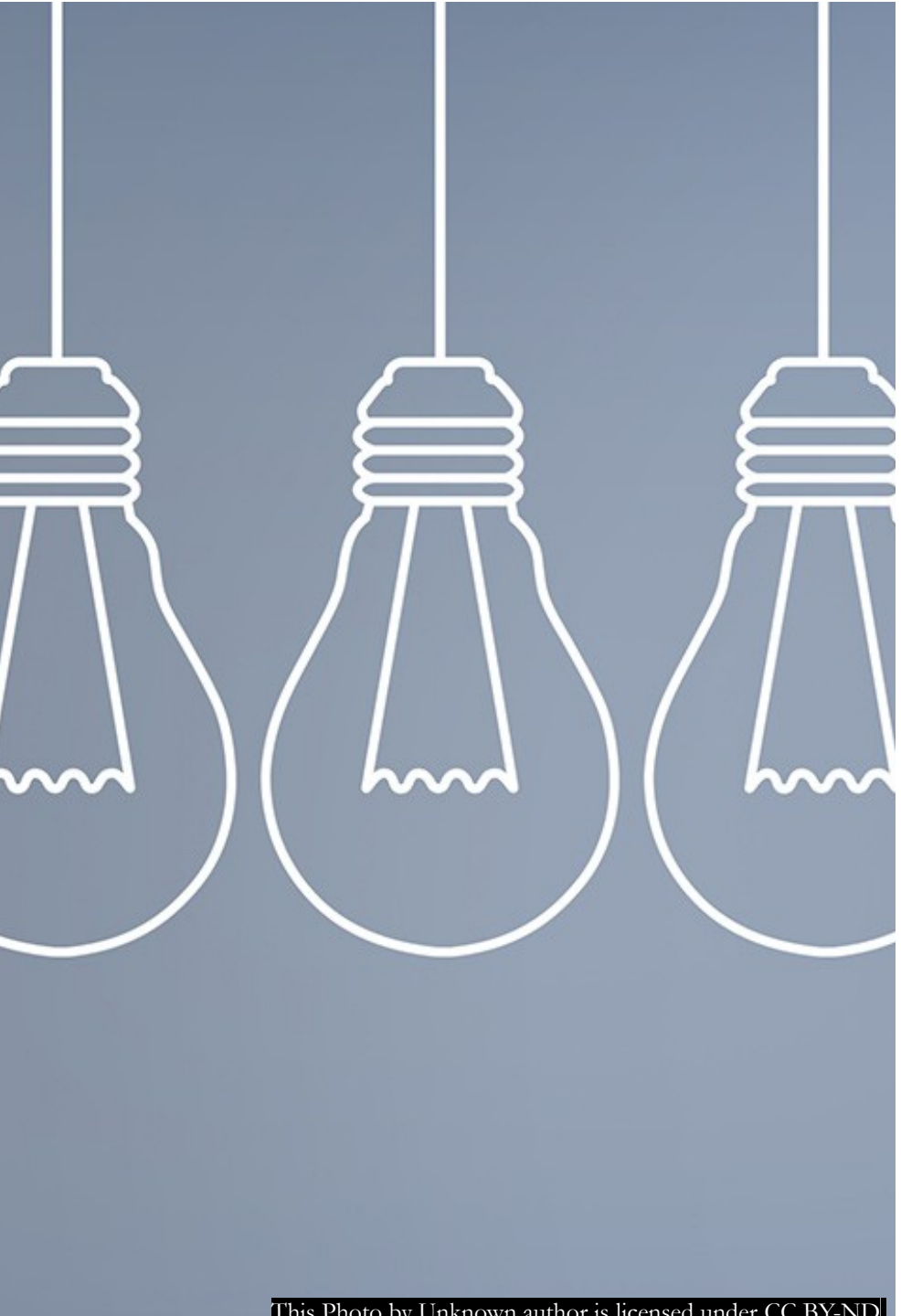
- **(3) Lack of MFA for Third Parties That Have Access to an Internal Network with Nonpublic Information:** Covered Entities that do not require third parties to use MFA when accessing their systems and the NPI on them often lead to the unauthorized access of sensitive consumer information.
- **(4) MFA Setups and Rollouts That Are Not Completed for All Users In a Timely Manner:** An MFA setup or rollout that is incomplete or slow can leave gaps in MFA coverage, without the direct oversight of one or more designated individuals

(c) 2023 Lexeprint Inc. All Rights Reserved.



# Proposed Changes to the NYDFS Cybersecurity Regulation

(c) 2023 Lexeprint Inc. All Rights Reserved.


This Photo by Unknown author is licensed under CC BY-ND

# Proposed Changes

- In late 2022, the NYDFS release its proposed amendments to the Part 500 Cybersecurity Regulations.
- The changes would be a meaningful development to the existing regulations:
  - Redesign of risk assessment process,
  - New technologies for system penetration testing,
  - Increased involvement of senior management, and
  - Notification of the NYDFS of unauthorized access.
- The changes will be meaningful to businesses as their compliance models will have to be significantly adapted, and their senior management potentially restructured.

(c) 2023 Lexeprint Inc. All Rights Reserved.


This Photo by Unknown author is licensed under CC BY-ND

# Policies and Procedures Requirements

- The proposed rules would expand the requirements for written policies and procedures to be more detailed and specific.
  - Section 500.5 would be at minimum require annual:
    - Penetration testing,
    - Automated scans of information systems,
    - Monitoring and notifying of emerging vulnerabilities,
    - Timely remediation of vulnerabilities, and
    - Document and report material issues to Board of Directors and senior management.

(c) 2023 Lexeprint Inc. All Rights Reserved.



# Technical Requirements

- The proposed amendments would introduce numerous technical requirements, including:
  - Limiting user access privileges and privileged accounts, reviewing access privileges annually, disabling remote device control protocols, and promptly terminating access following departures.
  - MFA requirements for remote access to covered information systems and entities.
  - Controls against malicious code and security awareness.
  - Expanded incident response plans to contain proactive and mitigating measures, business continuity, and disaster recovery plans.
  - Requirement for Class A companies to implement privileged access management solutions and automated blocking of commonly used passwords for all accounts.

(c) 2023 Lexeprint Inc. All Rights Reserved.

# How Do Executive Leadership and the Board Shape Corporate Cybersecurity Culture?

# Is There a Gap Between the Responsibility and the Expertise?

(c) 2023 Lexeprint Inc. All Rights Reserved


This Photo by Unknown author is licensed under CC BY-ND

# CISO Requirements

- CISO role:
  - The proposed regulations seek to address the limitations in visibility and authority that CISOs face in fulfilling their role by including the requirement that they have "the ability to direct sufficient resources to implement and maintain a cybersecurity program."
  - CISOs would also be required to report incidents in a timely manner.

(c) 2023 Lexeprint Inc. All Rights Reserved.


This Photo by Unknown author is licensed under CC BY-ND

# Senior Management Requirements

- The proposed regulations would shift the responsibility of administering and enforcing a company's cybersecurity program from the CISO with senior officers to the 'senior governing bodies.'
- These bodies would be responsible for approving the required policies and procedures.
- In practice, board members and executives would be expected to have sufficient cybersecurity expertise.
- Equally, CISOs would have to belong to the 'senior governing bodies.

(c) 2023 Lexeprint Inc. All Rights Reserved.



# Enforcement

- The proposed amendments signal increased enforcement appetite.
  - Under revised Section 500.20(b), incidents that allow access to nonpublic information or result in non-compliance with the regulation could lead to liability if not corrected within 24 hours.
  - The amended rule also introduces 15 mitigating factors that may be taken into account when assessing any penalty for a violation of banking, insurance, or financial services law.

(c) 2023 Lexeprint Inc. All Rights Reserved.



# FTC Cybersecurity Enforcement Capabilities

(c) 2023 Lexeprint Inc. All Rights Reserved.



This Photo by Unknown author is licensed under CC BY-NC-ND.



# What is the Federal Trade Commission?

- The Federal Trade Commission (FTC) is a regulatory agency that enforces consumer protection laws and prevents unfair business practices.
- The FTC combats monopolies, scams, among other methods of unfair competition and makes rules about these subjects to establish antitrust laws.

(c) 2023 Lexeprint Inc. All Rights Reserved.



# FTC Enforcement Authority

- Under Section 5 of the FTC Act, the Commission can act against unfair or deceptive acts or practices if:
  - A practice is can cause substantial injury, the injury is avoidable by consumers, and the injury is not at the expense of the consumer 15 U.S.C. § 45(n); or
  - A practice is deceptive and is likely to mislead consumers and affect their decisions regarding a product or service.

(c) 2023 Lexeprint Inc. All Rights Reserved.



This Photo by Unknown author is licensed under CC BY-NC.

# What is the GLBA?

- The Gramm Leach-Bliley Act (GLBA), also known as the Financial Modernization Act of 1999, is a federal law that requires financial institutions to explain their information-sharing practices to their customers and safeguard sensitive data.
- The GLBA was mainly founded to repeal the *Glass-Steagall Act* of 1933 and allow financial institutions to offer services previously forbidden.

(c) 2023 Lexeprint Inc. All Rights Reserved.


his Photo by Unknown author is licensed under CC BY-SA.

# What is the GLBA?

- The GLBA requires banks to share their information-sharing practices with customers.
  - All information concerning information collection, selling, and sharing, must be disclosed.
  - All firms must allow their customers an "opt-out" option.
- Financial institutions must establish security controls to safeguard clients' nonpublic personal information from any events threatening data integrity and safety.
- The 3 key sections of the GLBA are:
  - Financial Privacy Rule
  - Safeguards Rule
  - Pretexting Provisions

(c) 2023 Lexeprint Inc. All Rights Reserved.



# Relationship between the FTC and the GLBA

- The FTC is one of the authorities that enforces the GLBA, along with the federal banking agencies such as the Fed and the OCC, other federal regulatory authorities such as the SEC, and state insurance authorities.
- Section 5 of the GLBA grants the FTC the authority to audit privacy policies to ensure they are applied fairly.
- The Dodd-Frank Act in 2010 transferred new rulemaking authority to the Consumer Financial Protection Bureau (CFPB).

(c) 2023 Lexeprint Inc. All Rights Reserved.


This Photo by Unknown author is licensed under CC BY.

# Safeguarding Rule

- The GLBA demands that organizations implement administrative, physical, and technical protections as safeguards.
  - It requires companies to develop a written information security plan for the protection of customer information.
  - The plan must be appropriate to the institution's "size and complexity."
    - Must consider the nature of its activities and the sensitivity of its customer's information.

(c) 2023 Lexeprint Inc. All Rights Reserved.



# Amendments to the GLBA Safeguarding Rule

- The amendment Safeguard Rule requires financial institutions to develop and implement an information security program, that must be maintained continuously
- Some of the key amendments to the Safeguard Rule include:
  - There must be a designated person responsible for the Information Security Program, also known as a "qualified individual."
  - The program must be based on identified internal and external risk, through a written assessment.
  - Risk assessments testing the effectiveness and integrity of implemented safeguard are required.

(c) 2023 Lexeprint Inc. All Rights Reserved.



This Photo by Unknown author is licensed under CC BY-SA.

# Amendments to the GLBA Safeguarding Rule (cont.)

- Specific measures such as multifactor authentication, access controls for all customer information, and encryption of customer information on external networks must be implemented.
- Employee training is required to be updated based on evolving risk assessments.
- Third-party vendor selection and management.
- An incident response plan must be established if the organization maintains student information on 5000 or more consumers.

**National Law Review*

(c) 2023 Lexeprint Inc. All Rights Reserved.

# How to Corporations Protect Sensitive and Personal Data? What is their Responsibility Towards This Information?

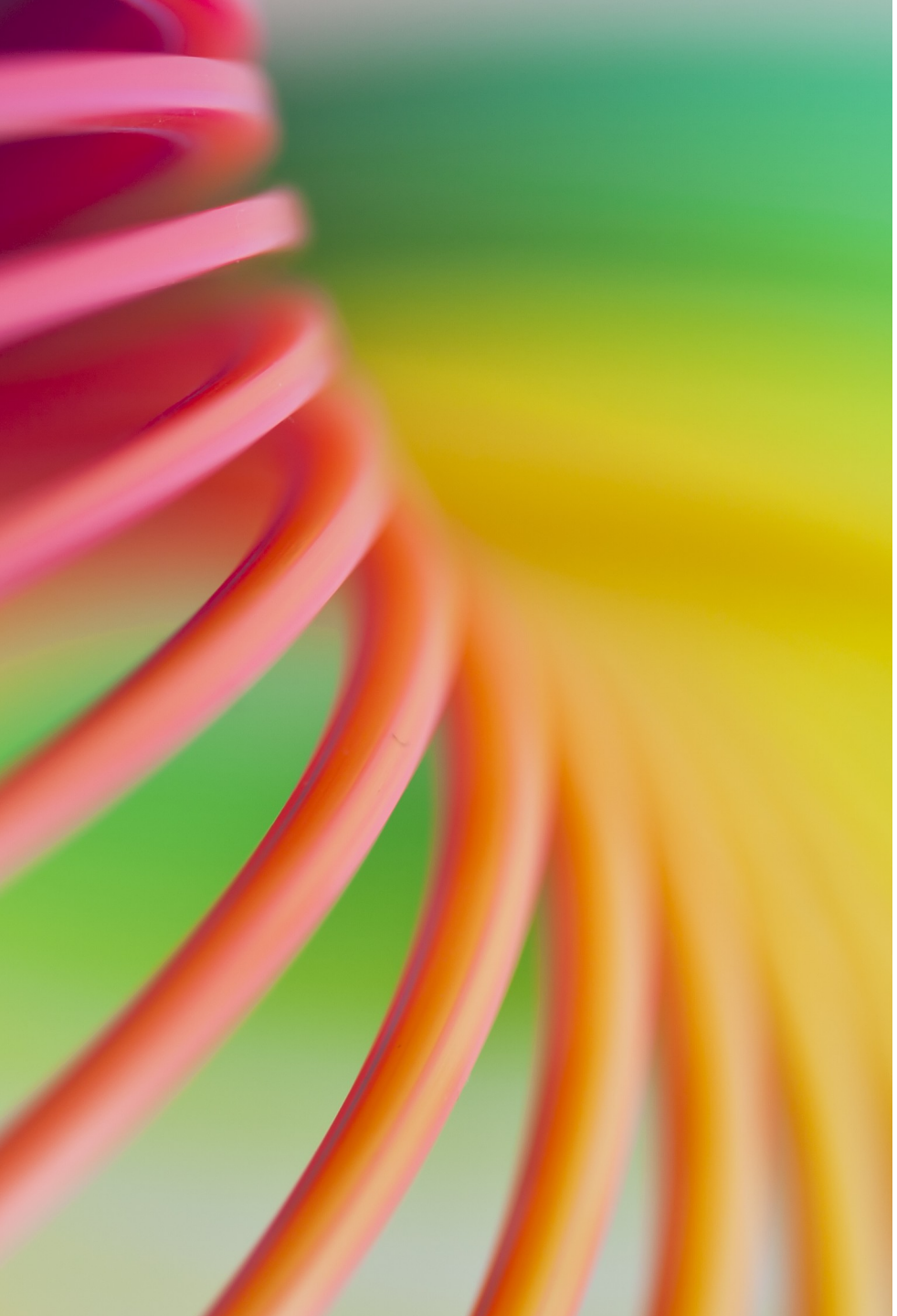
(c) 2023 Lexeprint Inc. All Rights Reserved



# Health Breach Notification (HBN) Rule

- In Sep 2021, the FTC clarified the scope of the HBN Rule and signaled intentions to begin enforcement.
- The Rule requires vendors of personal health records and related entities not covered by HIPAA to notify consumers and the FTC following a breach involving unsecured information.
- Makers of health apps, connected devices, and similar products must comply with the Rule.
- The notification requirements apply to breaches compromising Personal Health Record (PHR) identifiable health information.
- In the case of breaches involving 500 or more people, the rule requires notice to the media.

(c) 2023 Lexeprint Inc. All Rights Reserved.



# Children's Online Privacy Protection Rule

- The Children's Online Privacy Protection Rule (COPPA) imposes requirements on operators of websites or online services directed to children under 13 years
- COPPA also applies to online services that know they are collecting online personal information from children under 13.
- The Rule outlines three categories of information that must be disclosed on the online privacy policy of the websites.

(c) 2023 Lexeprint Inc. All Rights Reserved.

# Trade Regulation Rule on Commercial Surveillance and Data Security ANPR

(c) 2023 Lexeprint Inc. All Rights Reserved.


This Photo by Unknown author is licensed under CC BY-SA.

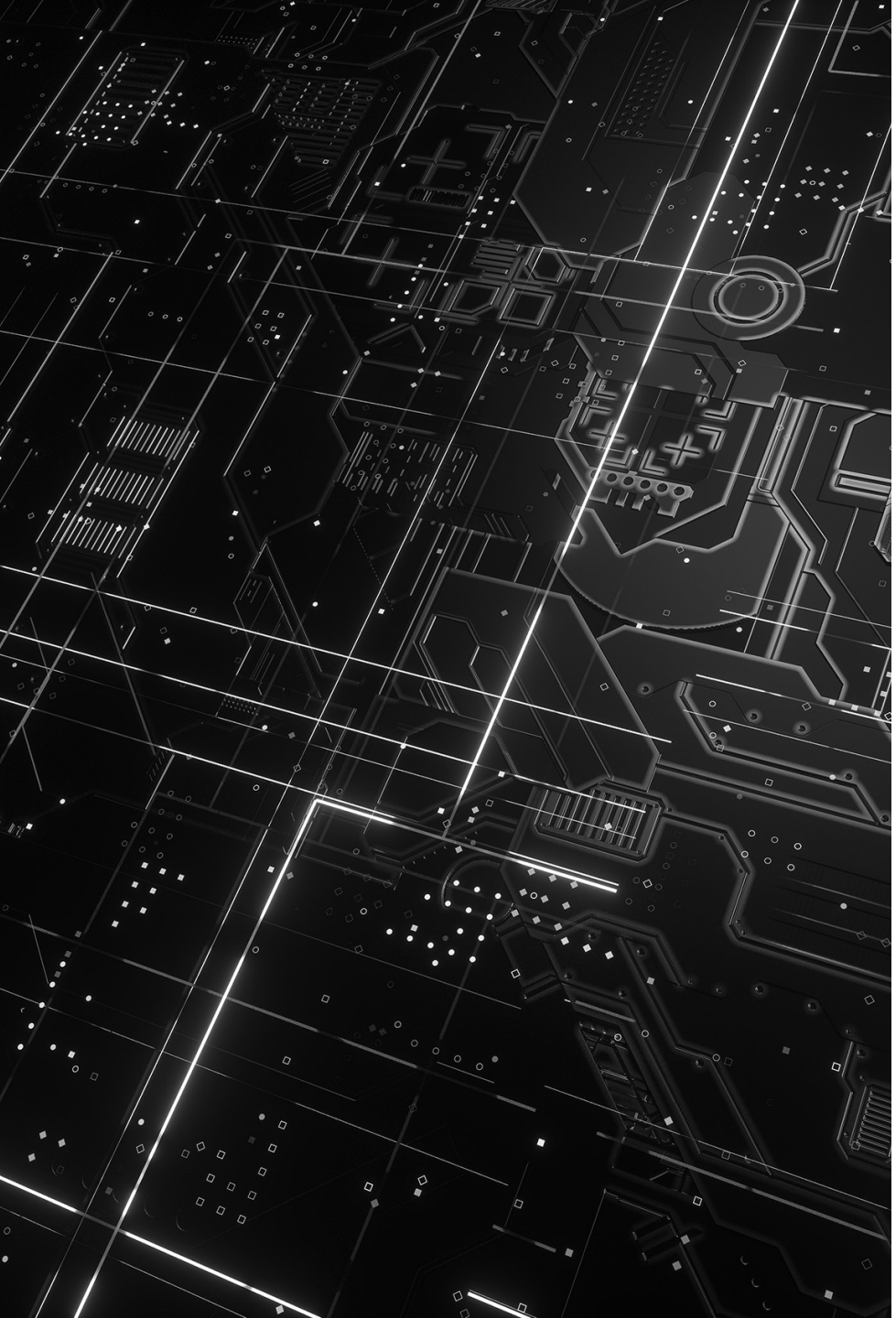
# FTC's Advance Notice on Proposed Rulemaking (ANPR)

- On August 11, 2022, the FTC announced it was seeking public comments on 95 questions on an ANPR for a Trade Regulation Rule on Commercial Surveillance and Data Security.

**16 CFR Part 464*

- After a review of the prevalence of commercial surveillance and lax data security practices, the FTC is seeking to enact new laws that protect consumers from discrimination and wrongful use of consumer data.
- While the period for public comment closed in the fall of 2022, the FTC is expected to:
  - Develop and publish the Final Rule
  - Submit it for Judicial Review

(c) 2023 Lexeprint Inc. All Rights Reserved.



# ANPR Definitions

- Commercial Surveillance
  - The collection and monetization of consumer data, often for marketing purposes.
- Data Security
  - The use of breach risk mitigation strategies, data management and retention measures, and breach notifications to protect data.

(c) 2023 Lexeprint Inc. All Rights Reserved.


This Photo by Unknown author is licensed under CC BY-SA.

# ANPR Invited Public Comment On Three Broad Themes

1. Understand the prevalence and effects of commercial surveillance and lax data security practices on consumers;

2. The economic effects of commercial surveillance and lax data security practices for consumers and competition; and

3. Plausible solutions for protecting consumers from commercial surveillance and lax data security practices.

**ANPR, pg. 24 of 44.*

(c) 2023 Lexeprint Inc. All Rights Reserved.



# Scope of ANPR's 94 Questions

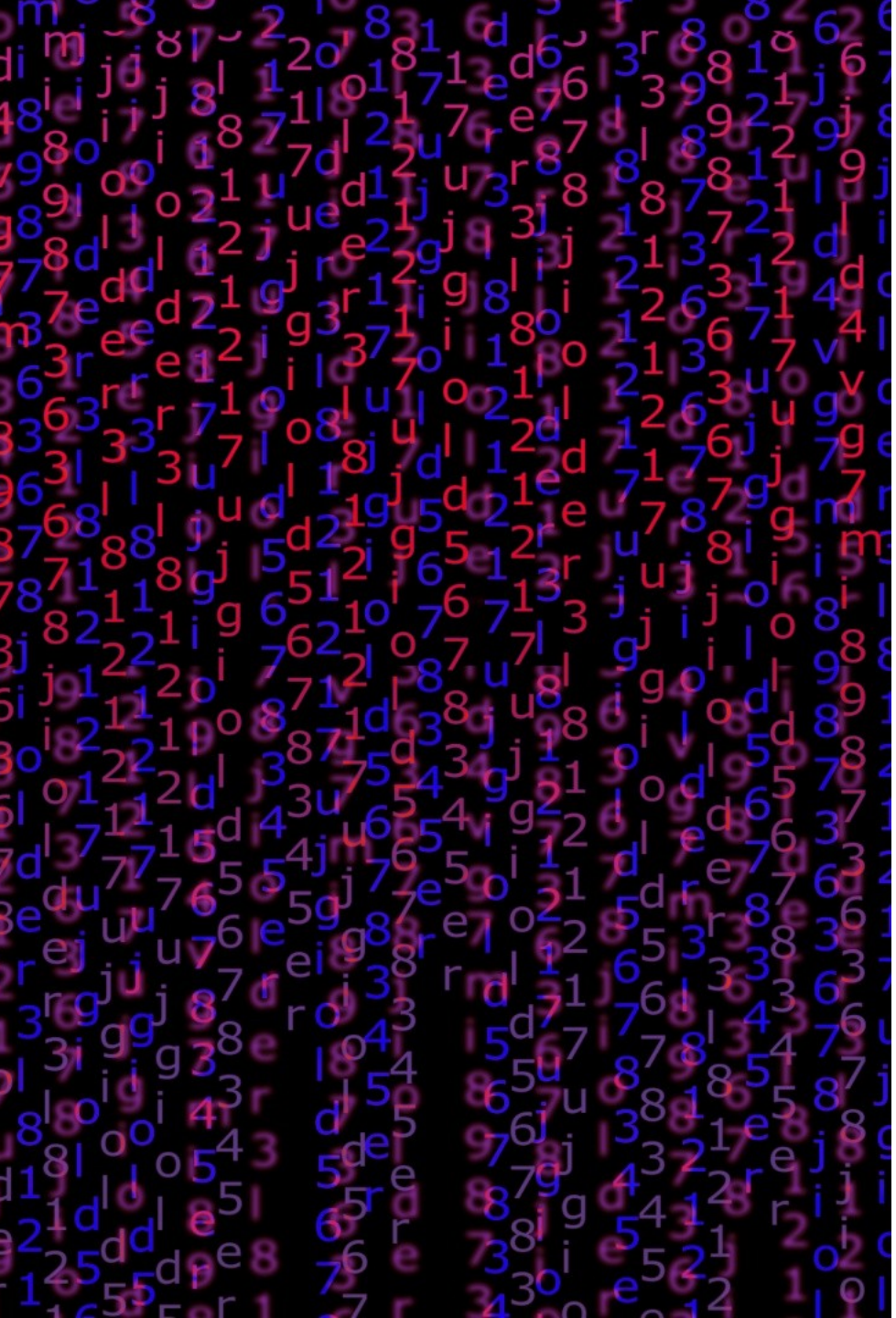
The FTC is sought information on the following:

- Harms to consumers from commercial surveillance and data security practices, including:
    - The FTC's ability to protect consumers from physical and psychological harms;
    - Measures used by companies to obtain and protect data; and
    - Suggestions on evaluating potential harms .
- Unique considerations for certain demographics, particularly children and protected classes, including:
    - Categorizing the use of children's data as unfair practice;
    - Marketing used for children and teens; and
    - The impact of discrimination against protected classes.

(c) 2023 Lexeprint Inc. All Rights Reserved.

# What Are Some of the Potential Risks of Increased AI Use and Implementation?

(c) 2023 Lexeprint Inc. All Rights Reserved



# Scope of ANPR's 94 Questions (Cont.)

- Automated decision-making (including Artificial Intelligence or Machine Learning (AI/ML)) caused errors, bias, and discrimination:
  - The prevalence of algorithmic error; and
  - Measures taken to address and prevent errors.
- Consumer consents and notices/disclosures to consumers about commercial surveillance and data security practices:
  - Effectiveness of consumer consent notes; and
  - Whether standards should be tailored to specific consumer groups.

(c) 2023 Lexeprint Inc. All Rights Reserved.



# Scope of ANPR's 94 Questions (Cont)

- How best to regulate these practices:
  - Whether the Commission should create a Section 18 rulemaking on commercial surveillance and data security; and
  - An evaluation on the effectiveness of self-regulation.
- Cost-benefit and trade-off considerations of a proposed rulemaking:
  - Potential disadvantages and benefits of a rulemaking;
  - How the rulemaking may quantify trade-offs; and
  - Whether companies should be held to different standards based on size or nature of the consumer data the company collects.

(c) 2023 Lexeprint Inc. All Rights Reserved.



# FTC Seeks Significant Enforcement Power

- The ANPR states that the enforcement of regulation of privacy and data security has been "insufficient to protect consumers from significant harms."
- Moreover, the ANPR explains that the FTC has had limited influence in preventing harmful corporate behavior and should pursue rules authorize monetary penalties without causing financial injury to consumers.
- The ANPR could "foster a greater sense of predictability for companies and consumers [and simultaneously limit] the uncertainty that case-by-case enforcement may engender."

(c) 2023 Lexeprint Inc. All Rights Reserved.



# *West Virginia v. EPA* (SCOTUS) 2022

- **Facts:** In 2015 the EPA proposed the Clean Power Plan (CPP) that added emission reduction regulations for existing powerplants A number of states and organizations contested the EPA's authority to do so.
- **Issue:** Does the Environmental Protection Agency have the authority to broadly regulate greenhouse gas emissions?
- **Ruling:** The Court indicated that, under the "major questions doctrine," in certain cases regulatory agencies could not issue rules affecting "a significant portion of the American economy" without "clear congressional authorization."
- **Relevance:** The Supreme Court's decision to limit the EPA's ability the scope of regulatory power may also limit the authority of the FTC to issue rules on data privacy. It puts into question the FTC's ability to pass its final rules under judicial review.

(c) 2023 Lexeprint Inc. All Rights Reserved.



# *LabMD, Inc. v. FTC* (11th Cir) 2018

- **Facts:** After a billing manager at LabMD made the contents of the "My Documents" folder to her computer for sharing, she exposed the contents of the files to users outside of the company through the software LimeWire. The FTC investigated the company's data leak and issued an administrative complaint against LabMD.
- **Issue:** Was the FTC's consent order unenforceable because it did not direct LabMD to cease committing an unfair act or practice within the meaning of Section 5(a)?
- **Ruling:** The Eleventh Circuit ruled that the FTC's consent order against LabMD was unenforceable because the security program requirements were not specific enough.

(c) 2023 Lexeprint Inc. All Rights Reserved.



# *LabMD, Inc. v. FTC* (11th Cir) 2018

- **Relevance:**
  - The FTC must specify prohibitions on a particular act or practice when issuing orders and cannot simply command that a company restructure its practices without proper reasoning.
  - Companies may begin to challenge the FTC's authority to regulate their data practices as a result of LabMD's win.

(c) 2023 Lexeprint Inc. All Rights Reserved.




(c) 2023 Lexeprint Inc. All Rights Reserved.



**Daniel B. Garrie, Esq.**
Law & Forensics – Founder
JAMS – Neutral
Harvard – Faculty
**Contact:**
W: (855) 529-2466
E: daniel@lawandforensics.com
URL: www.lawandforensics.com

LAW & FORENSICS
A Global Legal Engineering Firm

B.A., Computer Science, Brandeis Uni.
M.A., Computer Science Brandies Uni.
J.D., Rutgers School of Law

Daniel Garrie is the Co-Founder of Law & Forensics LLC, Head of Computer Forensics and Cyber Security Practice Groups and has been a dominant voice in the computer forensic and cybersecurity space for over 20 years. Prior to Daniel's legal career, he successfully built and sold several technology start-up companies. Since co-founding Law & Forensics LLC in 2008, Daniel has built it into one of the leading boutique cybersecurity forensic engineering firms in the industry. Daniel has both a Bachelor's and a Master's Degree in computer science from Brandeis University, as well as a J.D. degree from Rutgers Law School. Daniel has led forensic teams in some of the most visible and sensitive cyber incidents in the United States.

Daniel regularly testifies as an e-discovery, cybersecurity and computer forensic expert witness, authoring forensic expert reports on multi-million-dollar disputes. His ability to perform complex investigations and effectively communicate the results to a jury has made him one of the most sought-after experts in the country. His testimony has been pivotal in a number of cases. Since 2008, Daniel has served as a Neutral and Special Master and in 2016, he joined JAMS as one of the organization's youngest Neutrals. At JAMS, Daniel serves as an Arbitrator, Forensic Neutral, and technical Special Master with a focus on cybersecurity, cyrptocurrency, and complex software and technology related disputes.

Daniel is well-published in the cybersecurity space, Editor-in-Chief of the Journal of Law & Cyberwarfare, author of more than 200 articles and books including, "Understanding Software, the Internet, Mobile Computing, and the Cloud. A guide for Judges", published by the Federal Judicial Center. He has been recognized by several United States Supreme Court Justices for his legal scholarship and is a trusted source and a thought leader for cybersecurity articles and opinions, being cited over 500 times to date.

(c) 2022 Lexeprint Inc. All Rights Reserved.



**John D'Agostino**
Dagger Consulting LLC – CEO
Coinbase – Senior Advisor
**Contact:**
E: john@daggerllc.net

John D'Agostino is the CEO of Dagger Consulting LLC as well as the Coinbase Institutional Lead for Advisory and Strategic Partnerships. Prior, John was the US Managing Director for Waystone Governance, the world's largest fund governance firm. There, John served on the global governance committee and served on the Board of Directors for several of the world's largest asset managers, including several of the largest digital asset funds in the United States.

Previously, John was a Managing Director at KPMG Consulting, where he was part of the firm's global leadership for the Finance and Hedge Fund consulting groups. While at KPMG, he provided operational and strategic advisory services across a variety of industries, including advising on the acquisition of the London Metals Exchange by the Hong Kong Stock Exchange.

John served as Vice President and Head of Strategy for the New York Mercantile Exchange, where he helped transition the floor to electronic trading and was part of the leadership team building out the core systems to accommodate co-location, quant and HFT volumes. He also led the effort to develop the first Middle East energy derivatives exchange in partnership with the Dubai Government. This work and John's role was chronicled as the subject of two NY Times best selling books, Rigged by Ben Mezrich and The Start Up Of You by Reid Hoffman.

A cum laude graduate of Williams College, John received a Master's degree in Business Administration from Harvard Business School. He also studied Politics, Philosophy and Economics at Oxford University. John has adjunct lecturer positions at Instead, MIT and Columbia Universities, where he teaches courses in Fintech and Governance. In 2019, John was named Chair of the UK Consulate's Financial Services Working Group.

(c) 2023 Lexeprint Inc. All Rights Reserved.



**Justin Herring**
Mayer Brown - Partner
**Contact:**
Email: jherring@mayerbrown.com
URL: https://www.mayerbrown.com/en/people/h/justin-herring?tab=overview

Justin Herring is a partner in Mayer Brown's New York office and a member of the Cybersecurity & Data Privacy, Financial Services & Regulatory Enforcement and Global Investigations & White Collar Defense practices. Prior to joining Mayer Brown he was Executive Deputy Superintendent of the Cybersecurity Division at the New York State Department of Financial Services (NYDFS). His arrival underscores Mayer Brown's continued expansion of its cybersecurity and regulatory enforcement offerings and sustained growth in New York.

Justin provides comprehensive representation and counseling on sophisticated cybersecurity matters, including global incident response, enforcement actions and related litigation, cyber monitorships and regulatory compliance. He also advises individuals and entities in the crypto and fintech sectors.

At NYDFS, Justin served as the first leader of the agency's Cybersecurity Division, itself a first-of-its-kind unit at a financial services regulator. NYDFS issued the nation's first cybersecurity regulation for financial services, which has since become a model for other regulators such as the Federal Trade Commission, the Securities and Exchange Commission, and dozens of state banking and insurance regulators. Under Justin's leadership, NYDFS' Cybersecurity Division became a go-to source for guidance on novel and emerging cyber challenges. Among the influential regulation developed during his tenure was the creation of the nation's first cybersecurity regulation for financial services, and others adopted by the Federal Trade Commission and dozens of state banking and insurance regulators.

Justin also worked extensively on crypto and other innovation issues at NYDFS, including artificial intelligence. He served on NYDFS's Virtual Currency Licensing Committee, which approved all licenses granted to crypto companies. The Cybersecurity Division was also responsible for the cybersecurity and IT reviews for all license applications and examinations.

Prior to NYDFS, Justin served as the inaugural chief of the Cybercrimes Unit at the US Attorney's Office for the District of New Jersey, where he led several of the most consequential cyber prosecutions, including the first major insider trading and hacking cases (Newswire & SEC EDGAR Hacks) and the prosecution of the first ransomware ring focused on corporate extortion (Samsam). He served for nine years as an Assistant United States Attorney in the New Jersey and in the District of Maryland. In addition to complex cybercrimes prosecutions, Justin prosecuted financial crimes such as securities fraud and tax evasion. He has extensive courtroom experience, and has tried seven cases to verdict.

Justin served on the New York Governor's Cybersecurity Advisory Board from 2019 to 2022, where he developed guidance and solutions related to election security, critical infrastructure protection, and pandemic benefits fraud.

Earlier in his career, Justin clerked for Chief Judge Danny J. Boggs of the US Court of Appeals for the Sixth Circuit.

(c) 2023 Lexeprint Inc. All Rights Reserved.



**Paul Luehr**
Manatt - Partner
**Contact:**
E: pluehr@manatt.com
URL: https://www.manatt.com/

With three decades of experience across law, government and consulting, Paul Luehr is a respected technology leader who has handled some of the largest data security and privacy incidents in history. Throughout his career, Paul has been a trusted partner for organizations looking to optimize their privacy and data security practices. His work advising a wide range of clients—including national retailers, global financial institutions, digital health care organizations, web hosting companies, universities and manufacturers—gives him a unique understanding of the complex cybersecurity challenges and opportunities organizations face, as well as how to implement effective policies to mitigate crises and meet legal, technology and business needs.

In the privacy arena, and drawing on his notable consulting and regulatory experience, Paul advises companies on the Health Insurance Portability and Accountability Act (HIPAA), the General Data Protection Regulation (GDPR), new U.S. state privacy laws, and Federal Trade Commission (FTC) regulations. He draws on his roles as a regulator and litigator with the FTC, where he led the first cross-agency Internet team, and he provides a practical perspective on how to operationalize compliance obligations to clients across the nation.

On the cybersecurity side, Paul is consistently recognized as a top incident response attorney, and he spent over a decade with a global consulting firm where he led security experts into some of the largest breaches on record. He also prosecuted major cybercrimes for the U.S. Department of Justice and has unique experience providing advice related to ransomware gangs, wire fraud and business email compromises (BECs), distributed denial of service (DDoS) attacks, credential stuffing, structured query language (SQL) injections, and other digital hacks.

Over his career, Paul has managed complex digital forensics matters, led numerous investigations, argued cases at trial and on appeal, and represented clients before many regulators (e.g., HHS OCR, State Attorneys General, state Insurance Commissioners, the SEC, CISA and foreign data protection authorities (DPAs)). He has created robust compliance programs and frequently advised Board Directors and officers on new privacy and cybersecurity risks and obligations. He also has broad experience addressing artificial intelligence (AI), including performing cyber due diligence on mergers involving robotics and medical devices, and addressing new AI uses in financial services.

(c) 2023 Lexeprint Inc. All Rights Reserved.