



What NY Attorneys (and Everyone Else) Need to Know: Privacy, Cybersecurity, and Data Protection

October 2, 2023



Presenters



Colin J. Zick

*Partner and Co-Chair,
Privacy & Data Security Practice Group*

czick@foleyhoag.com

617-832-1275



Christopher Escobedo Hart

*Partner and Co-Chair,
Privacy & Data Security Practice Group*

chart@foleyhoag.com

617-832-1232

Today's Agenda

1

High-level overview of regulation and important points related to both cybersecurity and data privacy law

- Cybersecurity, Data Privacy: Core concepts
- Federal and state regulation
- Forthcoming updates to the NY "Cyber Regs"

2

Preparing for legal changes

**NY Cybersecurity CLE is available to today's attendees.
Today's presentation will be recorded!**

Cybersecurity, Data Privacy: Core Concepts

■ **Cybersecurity:** *Core Concepts*

- Preventing security breaches
- Identifying and patching system vulnerabilities
- Identifying attacks and attackers
- Maintaining system integrity
- Ensuring technical systems remain available to intended users

■ **Data Privacy:** *Core Concepts*

- Ensuring user information is properly processed (e.g., collected, used, stored, and shared)
- Limiting the collection of data and the potential uses of any data collected;
- Recognizing individuals' rights surrounding personal information, such as notice and consent

All of these concepts relate to your daily practice of law.

Federal Regulation: *Cybersecurity*

- At the federal level, regulation of both cybersecurity and data privacy reflect a fragmented patchwork of statutory and case law
- For cybersecurity, there are various standards in this patchwork, ranging between use of “reasonable” measures to areas of greater specificity
- It all started with Computer Fraud and Abuse Act (CFAA), 18 U.S.C. § 1030
 - First enacted in 1986
 - Original goals: Address computer hacking
 - ✦ *Criminal Liability*: Update existing tools for criminal prosecution (such as mail and wire fraud) for the new “cyber” era in the 1980s
 - ✦ *Civil Liability*: Extend existing tort law to provide new right of action
 - Prohibits individuals from intentionally (or knowingly) “accessing a computer”:
 - ✦ “without authorization”; or
 - ✦ “exceeding authorized access”
 - Can impose both **criminal** and **civil liability**
 - (Previously) a tool frequently used by the DOJ to prosecute hackers

CFAA: *Criminal Liability*

- Earlier cases -- *United States v. Morris* (1991), *United States v. Swartz* (2011), *United States v. Nosal* (2012) -- highlighted the federal government's use of CFAA to impose criminal liability for activities it deemed as "hacking"
- Turning point: *Van Buren* decision in 2021
 - SCOTUS limited the scope of conduct that could be criminally prosecuted under the "exceeds authorized access" prong of the CFAA
 - "To top it all off, the Government's interpretation of the statute would attach criminal penalties to a breathtaking amount of commonplace computer activity."
- **Future Enforcement**
 - 2022 Statement by DOJ:
 - ✦ DOJ will not bring cases under theories of "exceeds authorized access" unless such prosecution aligns with DOJ's goals, including to "promote privacy and cybersecurity by upholding the legal right of individuals, network owners, operators, and other persons to ensure the confidentiality, integrity, and availability of information stored in their information system"

CFAA: Civil Liability

■ *hiQ Labs v. LinkedIn*

- Arose from hiQ's practice of “scraping” data from LinkedIn profiles
- LinkedIn sued, bringing multiple claims, including civil liability under California’s state-level “CFAA” equivalent
- Litigated for multiple years; private settlement in 2022
- Further narrowed the scope of application of the CFAA as a tool for civil liability
- In light of *Van Buren*, there is limited ability to use the CFAA as a remedy against unwanted access to public websites

Other Specialized Federal Security Statutes: *Healthcare*

- Federal data security law is most advanced in specialized areas, such as health care, where HIPAA and FTC regulations cover a wide swath of information.
- What is HIPAA?
 - The Health Insurance Portability and Accountability Act of 1996 and subsequent regulations
 - Earliest example of specialized federal data security regulation
 - HIPAA is a major source of enforcement activity, primarily on the civil side; FTC enforcement in this area is growing
 - Lawyers can be governed by HIPAA, as “business associates” to “covered entities”
 - Here are the 2023 HIPAA investigations regarding hacking in just New York, in the last two months:

Breach Report Results							
Expand All	Name of Covered Entity ↕	State ↕	Covered Entity Type ↕	Individuals Affected ↕	Breach Submission Date ↕	Type of Breach	Location of Breached Information
🔍	Enzo Clinical Labs, Inc.	NY	Healthcare Provider	1700	08/31/2023	Hacking/IT Incident	Network Server
🔍	SUNY at Buffalo School of Dental Medicine	NY	Healthcare Provider	765	08/16/2023	Hacking/IT Incident	Network Server
🔍	VNS Health Plans	NY	Health Plan	103775	08/14/2023	Hacking/IT Incident	Network Server
🔍	Parsley Health, Inc.	NY	Business Associate	1004	07/07/2023	Unauthorized Access/Disclosure	Network Server
🔍	Quatela Center for Plastic Surgery	NY	Healthcare Provider	1085	06/20/2023	Unauthorized Access/Disclosure	Email
🔍	Enzo Clinical Labs, Inc.	NY	Healthcare Provider	2470000	06/05/2023	Hacking/IT Incident	Network Server
🔍	CareNet Medical Group, PC	NY	Healthcare Provider	10059	06/02/2023	Hacking/IT Incident	Network Server
🔍	Maimonides Medical Center	NY	Healthcare Provider	33000	06/01/2023	Hacking/IT Incident	Network Server
🔍	North Shore Medical Labs	NY	Healthcare Provider	500	05/26/2023	Hacking/IT Incident	Network Server
🔍	Albany ENT & Allergy Services, PC.	NY	Healthcare Provider	224486	05/25/2023	Hacking/IT Incident	Network Server
🔍	Goodwill Industries of Greater New York and Northern NJ, Inc.	NY	Healthcare Provider	805	05/24/2023	Hacking/IT Incident	Email
🔍	Essen Medical Associates, P.C.	NY	Healthcare Provider	500	05/16/2023	Hacking/IT Incident	Network Server
🔍	Catholic Health System	NY	Healthcare Provider	12759	05/11/2023	Unauthorized Access/Disclosure	Electronic Medical Record
🔍	University Urology	NY	Healthcare Provider	56816	05/01/2023	Hacking/IT Incident	Network Server

State Security Regulation

- Virtually all states have their own data security laws
- Most of these laws require reporting of data breaches to enforcement authorities (e.g., state Attorneys General, Offices of Consumer Affairs)
- These state laws may also require consumer notification, by various means
- State authorities are often overwhelmed by the volume of data breach reports

Other Security Considerations: *Ransomware*



- Beyond purely regulatory concerns, there are the practical concerns of protecting your data and that of your clients.
- The biggest single threat to that data is ransomware.
- What is **ransomware**?
 - A global intrusion campaign, often featuring state-sponsored actors.
 - Affecting public and private organizations around the world.
 - A formerly trusted event, business software updates, can be “trojanized” to distribute malware.
 - Emails that appear to be from clients or colleagues can be used to take over your account, through “phishing” attacks.
- Paying ransom **may not** always be the right answer
 - CFIUS concerns
 - Policy concerns

Other Security Considerations: *Ransomware (cont.)*

- Ransomware is big
 - From January to July 31, 2021, the Internet Crime Complaint Center (“IC3”) received 2,084 ransomware complaints with over \$16.8M in losses, a 62 percent increase in reporting and 20 percent increase in reported losses compared to the same time frame in 2020. Source: www.cisa.gov
 - During the first half of 2022, there were a total of 236.1 million ransomware attacks worldwide. Overall, the number of ransomware attacks decreased rapidly between the second and fourth quarters of 2021, going from nearly 189 million cases to 133 million. Source: www.statistica.com
 - Ransomware attacks resurged in early 2023:
 - ◆ new players such as Royal, BianLian, and Play ransomware gangs joined the field and major players like Lockbit and Clon executed mass-ransomware attacks.
 - ◆ The top targeted industries were manufacturing (19.5%), professional, scientific and technical services (15.3%) and educational services (6.1%). Source: <https://blackkite.com/whitepaper/ransomware-threat-landscape-2023/>

Federal Regulation: *Data Privacy*

- No comprehensive federal privacy law
 - **Proposed Legislation:** American Data Privacy and Protection Act (ADPPA), H.R. 8152
- Section 5 of the FTC Act
 - Prohibits “**unfair and deceptive**” acts or practices in or affecting commerce”
 - FTC as primary enforcement agency on federal level
 - Recent shift to increased enforcement action by Consumer Financial Protection Bureau (CFPB)

- Patchwork of different federal laws
 - Health Insurance Portability and Accountability Act (HIPAA)
 - ◆ Health Information Technology for Economic and Clinical Health Act (HITECH)
 - Children’s Online Privacy Protection Act (COPPA)
 - Gramm-Leach-Bliley Act (GLB)
 - ◆ Privacy Rule
 - ◆ Safeguards Rule
 - Fair Credit Reporting Act (FCRA)
 - Family Educational Rights and Privacy Act (FERPA)

State-Level Regulation:

Data Privacy

- States passing comprehensive consumer privacy bills (influenced by EU data protection laws):
 - California
 - Colorado
 - Connecticut
 - Delaware
 - Indiana
 - Iowa
 - Montana
 - Oregon
 - Tennessee
 - Texas
 - Utah
 - Virginia

- In the absence of comprehensive federal regulation, states are filling the regulatory gaps.
- 4 other states with active bills
 - California
 - At the forefront
 - Several states have modeled their own statutes after the California CCPA and CPRA

State-Level Data Privacy: *California*

■ California Consumer Privacy Act (CCPA), 2018

- Applies to for-profit businesses that do business in California and meet any of the following:
 1. Have a gross annual revenue of over \$25 million;
 2. Buy, sell, or share the personal information of 100,000 or more California residents, households, or devices;
or
 3. Derive 50% or more of their annual revenue from selling California residents' personal information.
- Overview of consumer rights:
 - ✦ The **right to know** about the personal information a business collects about consumers and **how it is used and shared**;
 - ✦ The **right to delete** personal information collected from consumers (with some exceptions);
 - ✦ The **right to opt-out** of the sale or sharing of consumers' personal information; and
 - ✦ The **right to non-discrimination** for exercising consumers' CCPA rights.
- Also governs the flow of information from covered business to service providers
- Also includes data breach notification requirements

State-Level Data Privacy: *California (cont.)*

- California Privacy Rights Act (CPRA), 2020
 - Amended the CCPA, including by providing additional rights to consumers:
 - ◆ **The right to correct** inaccurate personal information that a business has about consumers; and
 - ◆ The **right to limit the use and disclosure** of sensitive personal information collected about consumers.
 - Established the California Privacy Protection Agency

New SEC Rules

■ Rule 10

- Imposes new cybersecurity requirements on “Market Entities,” and a subset of those entities defined as “Covered Entities”
- Four major requirements
 - ✦ Cybersecurity policies
 - ✦ Notification and Reporting
 - ✦ Public Disclosure
 - ✦ Recordkeeping

■ Regulation SCI Amendments

- Expands the scope of entities covered by the rule
- Adds a host of new requirements

■ Regulation S-P Amendments

- Incident Response Program
- Customer Notification
- Expands scope of covered information
- Expands rule to transfer agents
- Recordkeeping

What Disclosures do the SEC Require?

Governance and Oversight

- How the Board is informed of cyber risks and incidents.
- How the Board integrates cyber risk and incident response into its overall risk management framework

Risk Assessment and Management

- How management establishes and implements cybersecurity policies and procedures.
- Management's role and expertise in uncovering, assessing, and addressing cyber risks
- Incident response

SEC Cybersecurity Risk Management, Strategy, Governance, & Incident Disclosure Rule



- Requires 8-K disclosure within four days of determination that a material cybersecurity incident has occurred
 - No permitted delays due to ongoing investigations or conflicting laws
- Cybersecurity incident update disclosures on
 - Material updates to previous cybersecurity incident disclosures
 - Previously undisclosed individually immaterial cybersecurity incidents that have become material in the aggregate
 - ✦ Information systems definition expanded to included systems owned or used
- Expanded governance disclosures in 10-Ks regarding
 - Policies and procedures for identifying and managing cyber risks, including risks associated with third party providers and impacts on strategy and financial planning and results
 - Board oversight, including process to inform and consideration in business strategy, risk management, and financial oversight
 - Management's role in assessing and managing cyber risks and implementing related policies and procedures
- Disclosures regarding board
 - Cybersecurity expertise of member of the board
 - How the board is informed about cybersecurity risks and the frequency of discussions on this topic
 - Whether and how the board or board committee considers cybersecurity risks as part of its business strategy, risk management, and financial oversight

SEC Cybersecurity Risk Management, Strategy, Governance, & Incident Disclosure Rule (cont'd)



■ Rule requirements

- Disclosure of a registrant's relevant policies and procedures
 - ✦ Benefit investors by providing transparency into the strategies and actions used to manage cybersecurity risks
 - ✦ Improve investors' understanding of the registrant's risk profile, including whether the registrant has a cybersecurity risk assessment program and undertakes activities designed to prevent, detect, and minimize effects of cybersecurity incidents
 - ✦ Enable investors to assess resiliency v. vulnerability for cybersecurity risks in the future
- Given that a significant number of cybersecurity incidents stem from third party service providers, the rule requires disclosures regarding selection and oversight of third-party entities
 - ✦ As proposed, 106(b) would require disclosure of whether the registrant
 - ▶ Has policies and procedures to oversee and identify cybersecurity risk associated with its use of any third party service provider (including, but not limited, to those that have access to customer and employee data), including
 - Whether and how cybersecurity considerations affect the selection and oversight of providers
 - What contractual mechanisms exist to mitigate cybersecurity risks related to providers
 - ▶ Undertakes activities to prevent, detect, and minimize cybersecurity incidents
 - ▶ Has undertaken to have previous cybersecurity incidents inform the registrant's governance, policies, procedures, and/or technologies.

New York Rules & Regulations

■ New York Stop Hacks and Improve Electronic Data Security (“SHIELD”) Act

- Strengthens New York’s breach notification law by:
 - ✦ Broadening the circumstances for when a breach needs to be reported.
 - ✦ Requiring any persons who own or license NY residents’ personal data to implement a “data security program” providing “reasonable safeguards” to protect that data.
- Gives AG enforcement authority; no private right of action.
- Who should be aware: NY-based entities and others who possess personal data from NY residents (particularly high volumes of sensitive data).

■ NYDFS Cybersecurity Regulations (23 NYCRR Part 500) (“NY Cyber Regs”)

- Outlines cybersecurity standards for financial companies in New York.
 - ✦ Companies must conduct risk assessments; maintain audit trails; dispose of data securely; limit access; develop a written cybersecurity policy; designate a Chief Information Security Officer; and abide by other best practices for cybersecurity.
 - ✦ Companies must report data security breaches to the Department within 72 hours of detection.
- Who should be aware: Any entity regulated by the NYDFS.

NY Cyber Regs: *Proposed Amendments*

■ Covered Entities

- The definition of “covered entity” remains largely the same under the proposed amendments
- Entity considered a “covered entity” if it is subject to licensing, registration, or other requirements under New York State’s Banking Law, Insurance Law, or Financial Services Law (even if regulated otherwise)
 - ✦ Special exemption for entities that would be considered a “covered entity” but are wholly-owned subsidiaries of another “covered entity” covered by the parent’s cybersecurity program
- Note that all companies (with some enumerated exceptions) engaged in the “business of selling or issuing checks” and the “business of receiving money for transmission or transmitting the same” (**READ: *money transmitters***) must be licensed pursuant to § 641(1) of the Banking Law, and thus may be considered a “covered entity”

NY Cyber Regs: *Proposed Amendments (cont.)*

■ Class A Companies

- Proposed amendments introduce a new class of regulated entity: “***Class A companies***”
- Defined as covered entities with at least \$20 million in gross annual revenue (across all affiliate entities) in New York State in each of the last two fiscal years, and either:
 - ✦ 2,000 employees (across all affiliate entities, regardless of location), or
 - ✦ Over \$1 billion in gross annual revenue (again, across all affiliate entities) in each of the last two fiscal years.
- If adopted in its current form, the proposed amendments will add the following heightened requirements for Class A companies (among others):
 - ✦ Conducting an independent audit (using internal or external auditors) of the company’s cybersecurity programs ***at least annually***;
 - ✦ Implementing an ***automated method of blocking commonly used passwords*** for all user accounts;
 - ✦ Implementing an endpoint detection and response solution to ***monitor anomalous activity***, along with a solution that centralizes logging and security event alerting.

Preparing for NY Compliance

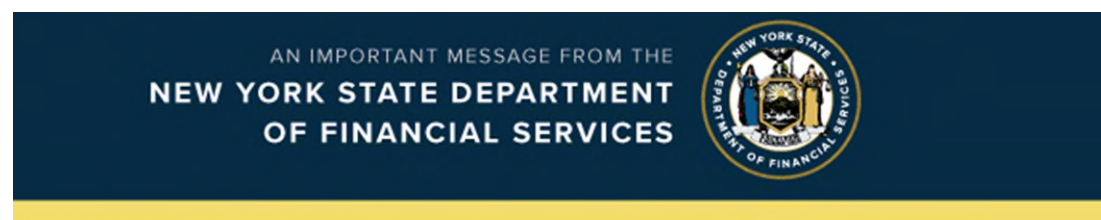
- **Annual Certification** (*amends current requirements*)
 - Covered entities must prepare and submit to NYDFS a “certification of compliance” either:
 - ✦ (i) confirming that the covered entity **materially** (*new addition in June 2023 revised draft*) complied with the regulation during the prior calendar year, or
 - ✦ (ii) acknowledging that the entity did not **fully** comply, identifying areas of **material** noncompliance and providing a timeline for remediation (or confirmation that remediation has been completed)
 - **Must be** signed by the covered entity’s “highest-ranking executive” and its CISO (or the senior officer responsible for the covered entity’s cybersecurity program in absence of a CISO)
 - ✦ **Note:** The June 2023 revisions specify that covered entities must designate a CISO within **one year** of the effective date
 - Covered entities must maintain all records, schedules, and other documentation supporting the certification for **five years**

Preparing for NY Compliance:

30 Days

- Covered entities will need to ensure that cybersecurity policies reflect the following:
 - **Ransomware.** In the event that a ransom payment is made in response to a ransomware attack, covered entities will need to:
 - ✦ Notify NYDFS within 24 hours of the payment; **and**
 - ✦ Provide NYDFS within 30 days of the payment with a written statement explaining why payment was made (in addition to other points).
 - **Notice of Cybersecurity Attack.** The proposed amendments retain the requirement to notify NYDFS within 72 hours of a cybersecurity event; however, the proposed amendments expand the list of types of cybersecurity events subject to this notice requirement and add in that covered entities must further:
 - ✦ **“Promptly”** provide any information regarding a cybersecurity event requested by NYDFS (in previous drafts, within 90 days – query what “promptly” means in practice).
 - ✦ Notify NYDFS within 72 hours of a cybersecurity event at the covered entity, the affiliates of the covered entity, or at a **third party service provider**.

NYDFS: Cybersecurity Event Notification



Date: **June 2, 2023**

To: **The Chief Information Security Officers of All Regulated Entities**

Subject: **MOVEit Transfer Vulnerability**

On June 1, 2023, the U.S. Department of Homeland Security's Cybersecurity and Infrastructure Security Agency ("CISA") and others announced that Progress Software ("Progress") released a security advisory for a vulnerability in MOVEit Transfer—a managed file transfer software.

All regulated entities should promptly assess risk to their organization, customers, consumers, and third party service providers based upon the evolving information and take action to mitigate risk. As you assess your risk, we recommend reviewing the [CISA Alert](#) and the [MOVEit Security Advisory](#).

Regulated entities are reminded to report cybersecurity events that meet the criteria of 23 NYCRR Section 500.17(a) as promptly as possible and within 72 hours at the latest via the secure DFS Portal, which can be accessed from DFS's [Cybersecurity Resource Center](#).

DFS considers evidence of unauthorized access to information systems, such as webshell installation, even if there has been no malware deployed or data exfiltrated, a reportable Cybersecurity Event pursuant to 23 NYCRR Section 500.17(a)(2).

One Year

- **CISO.** Covered entities will need to **designate a CISO**; defined as a “qualified individual responsible for overseeing and implementing the covered entity’s cybersecurity program and enforcing its cybersecurity policy”.
- **Backups.** Covered entities will need to maintain backups “**necessary to restoring material operations**” that are adequately protected from unauthorized alterations or destructions.
- **Written Incident Plans.** Covered entities will need to establish a written incident plan containing “proactive measures to investigate and mitigate cybersecurity events and ensure operational resilience”, and must include (1) incident response plans, (2) business continuity and disaster recovery plans (“**BCDR**”), and (3) disaster recovering plans. Covered entities must provide relevant training to all employees responsible for such plans and test the plans (specifically the incident response and BCDR plans) at least **annually**.
- **Written Encryption Policy.** Covered entities will need to implement written policies for encryption that meet “industry standards” to protect nonpublic information held or transmitted by the covered entity both in transit over external networks and at rest. Class A companies will have additional and heightened requirements.

Preparing for NY
Compliance:

Further Out

Eighteen Months

- **Scans.** Moving forward, covered entities will need to conduct annual automated scans of information systems (and manually review systems not covered by automated scans) to analyze and report on vulnerabilities.
- **Malicious Code Protection.** Covered entities will need to implement controls that protect against malicious code (including monitoring and filtering web traffic and emails).

Two Years

- **Asset Inventory.** Covered entities must implement written policies and procedures designed to “ensure a complete, accurate and documented asset inventory”.
- **Multi-Factor Authentication (“MFA”).** Covered entities will need to use MFA for (1) remote access to information systems, (2) remote access to third-party applications (including cloud-based applications), and (3) all privileged accounts

Preparing for NY
Compliance:

Further Out (cont.)



FOLEY
HOAG

CLE CODE: FH2023

CLE approved in NY and CA

Please direct all CLE requests to Robert Burke at rburke@foleyhoag.com.

Key Takeaways

- Privacy and security are distinct but interrelated.
- Both convergence and divergence: no single comprehensive law, but laws are trending toward similarity.
- Broad expertise required for appropriate risk management.
- Strong data protection strategies require strong internal management and governance.
- Increasingly active regulatory and enforcement space.

Questions?
