

Morgan Lewis

NEW YORK DEPARTMENT OF FINANCIAL SERVICES

CYBERSECURITY REGULATIONS

Charles Horn, Mark Krotoski, Melissa Hall, Sarah Riddell

April 5, 2017

Presenter: Charles Horn



- Partner in the investment management practice.
 - Member of the Morgan Lewis FinTech initiative.
- Counsels US and international banks and other financial institutions on corporate, regulatory, supervisory, enforcement, and compliance matters before all major federal and state financial regulatory agencies, and governance, structure, management, and operational matters.
- Advises clients on major federal financial services statutes and regulations, as well as on US and international financial reform developments.
- Represents technology-based or technology-reliant bank and nonbank financial services companies on regulatory, compliance, licensing, service relationship, and risk management matters.
- Editor of the Morgan Lewis *All Things FINREG* blog.

Phone: 202.739.5951, Email: charles.horn@morganlewis.com

Morgan Lewis

2

Presenter: Mark Krotoski



- Litigation partner in the privacy and cybersecurity and Antitrust practices.
- National Coordinator for the Department of Justice (DOJ) Computer Hacking and Intellectual Property (CHIP) Program in Washington, DC. and as a CHIP prosecutor in Silicon Valley, among other DOJ leadership positions.
 - Successfully led prosecutions and investigations of nearly every type of international and domestic computer intrusion, cybercrime, and criminal intellectual property case.
 - Proficient on foreign economic espionage cases involving the theft of trade secrets with the intent to benefit a foreign government.
 - He and his team successfully prosecuted two of the first foreign economic espionage cases authorized by DOJ under the Economic Espionage Act.
 - Developed and led DOJ training efforts on computer crimes, economic espionage, and the collection of electronic evidence during an investigation and admission into evidence at trial, among other related topics.
- Advises clients on developing effective Cybersecurity and Trade Secret Protection Plans and in responding to a data breach incident or misappropriation of trade secrets. He has written extensively on these issues.

Phone: 650.843.7212, Email: mark.krotoski@morganlewis.com

Morgan Lewis

3

Presenter: Melissa Hall



- Of counsel in the investment management practice
 - Member of the Morgan Lewis FinTech and Consumer Protection initiatives
- Represents US and overseas banks, nonbank financial services companies, investors in financial services, and technology companies in regulatory and corporate matters.
- Advises clients on a wide range of state and federal financial regulatory laws and regulations.
- Provides counsel on financial regulatory compliance and enforcement, including state and federal licensing requirements, consumer financial products and compliance, payment systems, corporate and transactional matters, financial institution investment and acquisition, and the development of new financial services products and fintech products.
- Represents clients before Federal Deposit Insurance Corporation (FDIC), the Office of the Comptroller of the Currency (OCC), the Federal Reserve Board of Governors, and the Consumer Financial Protection Bureau (CFPB), and state banking agencies.

Phone: 202.739.5883, Email: melissa.hall@morganlewis.com

Morgan Lewis

4

Presenter: Sarah Riddell



- Associate in the investment management practice.
- Advises domestic and foreign exchanges, derivatives clearing organizations, swap execution facilities, and other financial institutions on a broad range of regulatory matters, including US Commodity Futures Trading Commission (CFTC) registration and compliance, leveraging experience as a lawyer at the CFTC.
 - Guides CFTC applicants (including swap dealers, introducing brokers, commodity pool operators, and commodity trading advisors) through the registration process.
 - Counsels firms on relevant exemptions from CFTC registration on which they may rely.
 - Assists swap dealers and futures commission merchants with ongoing compliance obligations, including the requirement to submit to the CFTC an Annual Chief Compliance Officer Report.
- Provides guidance to financial institutions subject to cybersecurity requirements, including swap dealers, hedge funds, sponsors of exchange-traded funds, and banks.

Phone: 312.324.1154, Email: Sarah.Riddell@morganlewis.com

Morgan Lewis

5

Overview

- Background and Context
- The Final Rule
- Practical Considerations
- Responding to a "Cybersecurity Event"
- Q&A

Morgan Lewis

6

NY STATE DEPARTMENT OF FINANCIAL SERVICES CYBERSECURITY RULE

BACKGROUND & CONTEXT

Background and Context

- Other Federal and State Requirements
 - Increasing regulatory environment
 - Divergent standards
- NY State Department of Financial Services Cybersecurity Rule
 - March 1, 2017
 - Some provisions to be phased in
 - Final rule is an improved version of the proposed rule
 - Still stringent
 - Many novel standards
 - Many requirements are based on a risk assessment (= more tailored)

Morgan Lewis

8

Federal Laws Increasing Enforcement and Regulatory Scrutiny



- Federal Trade Commission
 - Section 5 (unfair and deceptive practices)
 - Gramm-Leach-Bliley Act Safeguards Rule (financial services)



- SEC
 - Reg S-P Safeguarding Rule
 - Reg S-P Disposal Rule
 - Cybersecurity Disclosures Guidance



- HHS Office for Civil Rights
 - Health Insurance Portability and Accountability Act (HIPAA)



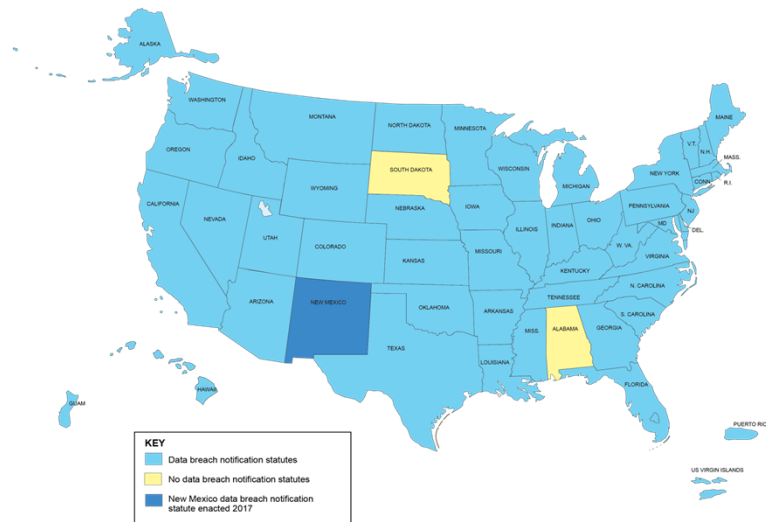
- Law Enforcement
 - DOJ
 - FBI, USSS



Morgan Lewis

9

State Data Breach Notification Statutes



Morgan Lewis

10

Civil Enforcement Fines and Consequences

- Fines
- Cease and desist
- Censure
- Injunctive action
- Establishing a comprehensive security program
 - Address security risks
 - Protect data
- Initial and biennial cybersecurity or data assessments
- Term of agency jurisdiction

Morgan Lewis

11

Proposed Rule



The screenshot shows the Department of Financial Services website. The main heading is 'Department of Financial Services'. Below it is a navigation bar with links: Home, ABOUT US, Consumers, Banking Industry, Insurance Industry, Legal, and Reports & Publications. Under 'ABOUT US' are links for Mission & Leadership, Initiatives, History, News Room, Who We Supervise, Careers with DFS, Contact Us, and Procurement. The 'News Room' section is active, showing a list of press releases from 2016 to 2011. The selected press release is dated September 13, 2016, and is titled 'GOVERNOR CUOMO ANNOUNCES PROPOSAL OF FIRST-IN-THE-NATION CYBERSECURITY REGULATION TO PROTECT CONSUMERS AND FINANCIAL INSTITUTIONS'. The text of the release states: 'Proposed Rule Aims to Protect Consumer Data and Financial Systems from Terrorist Organizations and Other Criminal Enterprises'.

“[A]nnounced that a new **first-in-the-nation regulation** has been proposed to protect New York State from the ever-growing threat of cyber-attacks. The regulation requires banks, insurance companies, and other financial services institutions regulated by the State Department of Financial Services to establish and **maintain a cybersecurity program** designed to protect consumers and ensure the safety and soundness of New York State’s financial services industry.”

procedures designed to ensure the security of information systems and nonpublic information accessible to, or held

Morgan Lewis

<http://www.dfs.ny.gov/about/press/pr1609131.htm>

12

Update and Delayed Implementation



Press Release

December 28, 2016

Contact: Richard Loconte, 212-709-1691



DFS ISSUES UPDATED PROPOSED CYBERSECURITY REGULATION PROTECTING CONSUMERS AND FINANCIAL INSTITUTIONS

First-in-the-Nation Proposed Rule Aims to Protect Consumer Data and Financial Systems from Terrorist Organizations and Other Criminal Enterprises

Financial Services Superintendent Maria T. Vullo today announced that the New York State Department of Financial Services (DFS) has updated its proposed first-in-the-nation **cybersecurity regulation** to protect New York State from the ever-growing threat of cyber-attacks. The proposed regulation, which will be effective March 1, 2017, will require banks, insurance companies, and other financial services institutions regulated by DFS to establish and maintain a

“The proposed regulation, which will be effective **March 1, 2017**, will require banks, insurance companies, and other financial services institutions regulated by DFS to establish and maintain a cybersecurity program designed to protect consumers and ensure the safety and soundness of New York State’s financial services industry.”

period, which ended on November 14, 2016, and has incorporated those suggestions that DFS deemed appropriate in an updated draft that will be subject to an additional final 30-day comment period. DFS will focus its final review on any new comments that were not previously raised in the original comment process.

The updated proposed regulation, which was submitted to the New York State Register on December 15, 2016 and published today, will be finalized following a 30-day notice and public comment period.

###

Morgan Lewis

<http://www.dfs.ny.gov/about/press/pr1612281.htm>

13

Comment Period



- December 28, 2017
- NY DFS:
 - “DFS carefully considered all comments submitted regarding the proposed regulation during the 45-day comment period, which ended on November 14, 2016, and has incorporated those suggestions that DFS deemed appropriate in an updated draft that will be subject to an additional final 30-day comment period. **DFS will focus its final review on any new comments that were not previously raised in the original comment process.**”

Morgan Lewis

Mark L. Krotoski
Partner
+1.609.443.7212
mark.krotoski@morganlewis.com

Charles Horn
Partner
+1.202.739.5851
charles.horn@morganlewis.com

January 27, 2017

VIA EMAIL: CyberRegComments@dfs.ny.gov

Maria T. Vullo, Superintendent
New York State Department of Financial Services
One State Street
New York, NY 10004-1511

Dear Superintendent Vullo:

We appreciate the opportunity to comment on the New York State Department of Financial Services’ (“DFS”) re-proposed regulatory framework titled “Cybersecurity Requirements for Financial Services Companies” (the “Supplemental Proposed Rules”).

On September 13, 2016, the DFS issued a set of proposed rules, described as “a new first-in-the-nation regulation.” After the first comment period closed on December 28, 2016, the DFS revised its Proposed Rules and delayed the effective date until March 1.¹ The Supplemental Proposed Rules would require banks, insurers, and other DFS-supervised financial services companies to adhere to stringent cybersecurity requirements mandating firms to test their systems, establish plans to respond to cybersecurity events, and annually certify compliance with the cybersecurity requirements, among other mandates.

We had previously commented on the first set of proposed rules; our comment letter is attached as *Appendix A*, and we welcome the opportunity to offer our suggestions to enhance the Supplemental Proposed Rules in this comment letter.


¹ See Press Release: Governor Cuomo Announces Proposal of First-In-The-Nation Cybersecurity Regulation To Protect Consumers and Financial Institutions (Sept. 13, 2016), available at <http://www.dfs.ny.gov/legal/regulations/proposed/pr500.pdf>; see also New York State Department of Financial Services Proposed 23 NYCRR 500, Cybersecurity Requirements For Financial Services Companies, available at <http://www.dfs.ny.gov/legal/regulations/proposed/pr500.pdf>.

² See Press Release: DFS Issues Updated Proposed Cybersecurity Regulation Protecting Consumers And Financial Institutions (Dec. 28, 2016), available at <http://www.dfs.ny.gov/about/press/pr1612281.htm>; see also New York State Department of Financial Services Proposed 23 NYCRR 500, Cybersecurity Requirements For Financial Services Companies, available at <http://www.dfs.ny.gov/legal/regulations/proposed/pr500.pdf>.

Morgan Lewis

14

Final Cybersecurity Regulation



Press Release


February 16, 2017

Contact: Richard Loconte, 212-709-1691

GOVERNOR CUOMO ANNOUNCES FIRST-IN-THE-NATION CYBERSECURITY REGULATION PROTECTING CONSUMERS AND FINANCIAL INSTITUTIONS FROM CYBER-ATTACKS TO TAKE EFFECT MARCH 1

Regulation Protects Consumer Data and Financial Systems from Terrorist Organizations and Other Cyber Criminals

Regulated Financial Institutions Must Establish and Maintain a Cybersecurity Program to Protect Consumers and the Industry



“The final risk-based regulation includes certain regulatory minimum standards while encouraging firms to keep pace with technological advances.”

Effective **March 1, 2017**

consumers and our financial system from the ever increasing threat of cyber-attacks,” **Governor Cuomo said.** “These strong, first-in-the-nation protections will help ensure this industry has the necessary safeguards in place in order to protect themselves and the New Yorkers they serve from the serious economic harm caused by these devastating cyber-crimes.”

New York State Department of Financial Services Superintendent Maria T. Vullo said, “With this landmark regulation, DFS is ensuring that New York consumers can trust that their financial institutions have protocols in place to protect the security and privacy of their sensitive personal information. As our global financial network becomes even more interconnected and entities around the world increasingly suffer information breaches, New York is leading the charge to combat the ever-increasing risk of cyber-attacks.”

Morgan Lewis

<http://www.dfs.ny.gov/about/press/pr1702161.htm>

15

NY STATE DEPARTMENT OF FINANCIAL SERVICES CYBERSECURITY RULE

THE FINAL RULE

The Final Rule: Overview

- Covered Entities/Exemptions
- Cybersecurity Event
- Attorney-Client Privilege
- Phased-In Implementation
- Cybersecurity Program/Policy
- Risk Assessment
- CISO
- New Notification Requirement
- Annual Compliance Certification
- Third Party Vendor Relationships
- Incident Response Plan
- Protection of Nonpublic Information
- Periodic Testing, Monitoring & Review
- Qualified Personnel & Training
- Audit Trail
- Liability for Noncompliance

Morgan Lewis

17

Covered Entities & Exemptions



- Who is covered?
- DFS Regulated Entities
 - Insurance
 - Financial Services
 - Banking or Financial Institutions
- "[A]ny Person operating under or required to operate under a license, registration, charter, certificate, permit, accreditation or similar authorization under the Banking Law, the Insurance Law or the Financial Services Law."

Morgan Lewis

[Section 500.01(c)]

18

Covered Entities & Exemptions



- Who is covered?
- DFS Regulated Entities
 - Insurance
 - Financial Services
 - Banking or Financial Institutions
- “[A]ny Person operating under or required to operate under a **license, registration, charter, certificate, permit, accreditation or similar authorization** under the **Banking Law**, the **Insurance Law** or the **Financial Services Law**.”

Morgan Lewis

[Section 500.01(c)]

19

Covered Entity Examples



- DFS Regulated Entities
- **Some Examples:**
 - Banks & Trust Companies
 - Bank Holding Companies
 - Credit Unions
 - Foreign Agencies
 - Foreign Bank Branches
 - Health Insurers
 - Licensed Lenders
 - Life Insurance Companies
 - Money Transmitters
 - Mortgage Bankers and Mortgage Brokers
 - Property and Casualty Insurance Companies
 - Safe Deposit Companies
 - Savings Banks and Savings & Loan Associations

Morgan Lewis

[Section 500.01(c)]

20

Exemptions



- Certain limited exemptions
- Notice of Exemption required
- Where exemption ceases
 - “as of its most recent fiscal year end”
 - “180 days from such fiscal year end to comply with all applicable requirements”

APPENDIX B (Part 500)

(Covered Entity Name) _____

(Date) _____

Notice of Exemption

In accordance with 23 NYCRR § 500.19(e), (Covered Entity Name) hereby provides notice that (Covered Entity Name) qualifies for the following Exemption(s) under 23 NYCRR § 500.19 (check all that apply):

☐ Section 500.19(a)(1)

☐ Section 500.19(a)(2)

☐ Section 500.19(a)(3)

☐ Section 500.19(b)

☐ Section 500.19(c)

☐ Section 500.19(d)

If you have any question or concerns regarding this notice, please contact:

(Insert name, title, and full contact information)

(Name) _____ Date: _____

(Title) _____

(Covered Entity Name)

[DFS Portal Filing Instructions]

Morgan Lewis

[Sections 500.19(e), (g)]

21

Exemptions



- “(b) An employee, agent, representative or designee of a Covered Entity, who is itself a Covered Entity, is exempt from this Part and need not develop its own cybersecurity program to the extent that the employee, agent, representative or designee is **covered by the cybersecurity program of the Covered Entity.**”

Morgan Lewis

[Section 500.19(b)]

22

Exemptions



- Persons subject to:
- Charitable Annuity Societies
 - Insurance Law section 1110
- Risk Retention Groups
 - Insurance Law section 5904
- Any accredited reinsurer or certified reinsurer that has been accredited or certified
 - Pursuant to 11 NYCRR 125

Morgan Lewis

[Section 500.19(f)]

23

Exemptions



- (1) **fewer than 10 employees**, including any independent contractors, of the Covered Entity or its Affiliates located in New York or responsible for business of the Covered Entity, **or**
 - (2) **less than \$5,000,000 in gross annual revenue** in each of the last three fiscal years from New York business operations of the Covered Entity and its Affiliates, **or**
 - (3) **less than \$10,000,000 in year-end total assets**, calculated in accordance with generally accepted accounting principles, including assets of all Affiliates
- Exempt from:
 - Section 500.04 [CISO]
 - 500.05 [Penetration Testing and Vulnerability Assessments]
 - 500.06 [Audit Trail]
 - 500.08 [Application Security]
 - 500.10 [Cybersecurity Personnel and Intelligence]
 - 500.12 [Multi-Factor Authentication]
 - 500.14 [Training and Monitoring]
 - 500.15 [Encryption of Nonpublic Information]
 - 500.16 [Incident Response Plan]

Morgan Lewis

[Section 500.19(a)]

24

Exemptions



- Covered Entity that does not directly or indirectly operate, maintain, utilize or control any Information Systems, **and**
- Not required to, directly or indirectly control, own, access, generate, receive or possess Nonpublic Information
- Exempt from:
 - Section 500.02 [Cybersecurity Program]
 - 500.03 [Cybersecurity Policy]
 - 500.04 [CISO]
 - 500.05 [Penetration Testing and Vulnerability Assessments]
 - 500.06 [Audit Trail]
 - 500.07 [Access Privileges]
 - 500.08 [Application Security]
 - 500.10 [Cybersecurity Personnel and Intelligence]
 - 500.12 [Multi-Factor Authentication]
 - 500.14 [Training and Monitoring]
 - 500.15 [Encryption of Nonpublic Information]
 - 500.16 [Incident Response Plan]

Morgan Lewis

[Section 500.19(c)]

25

Exemptions



- Captive Insurance Companies
 - Article 70 of the Insurance Law
- Covered Entity “does not and is not required to directly or indirectly control, own, access, generate, receive or possess Nonpublic Information other than information relating to its corporate parent company (or Affiliates)”
- Exempt from:
 - Section 500.02 [Cybersecurity Program]
 - 500.03 [Cybersecurity Policy]
 - 500.04 [CISO]
 - 500.05 [Penetration Testing and Vulnerability Assessments]
 - 500.06 [Audit Trail]
 - 500.07 [Access Privileges]
 - 500.08 [Application Security]
 - 500.10 [Cybersecurity Personnel and Intelligence]
 - 500.12 [Multi-Factor Authentication]
 - 500.14 [Training and Monitoring]
 - 500.15 [Encryption of Nonpublic Information]
 - 500.16 [Incident Response Plan]

Morgan Lewis

[Section 500.19(d)]

26

Cybersecurity Event



- “[A]ny act or attempt, successful or unsuccessful, to gain unauthorized access to, disrupt or misuse an Information System or information stored on such Information System.”
- Broad definition
 - Attempts
 - Even if unsuccessful
- “*Authorized User* means any employee, contractor, agent or other Person that participates in the business operations of a Covered Entity and is authorized to access and use any Information Systems and data of the Covered Entity.”
- “*Person* means any individual or any non-governmental entity, including but not limited to any nongovernmental partnership, corporation, branch, agency or association.”
- Legal Conclusion

Morgan Lewis

[Sections 500.01(b), (d), (i)]

27

Role of Attorney-Client Privilege

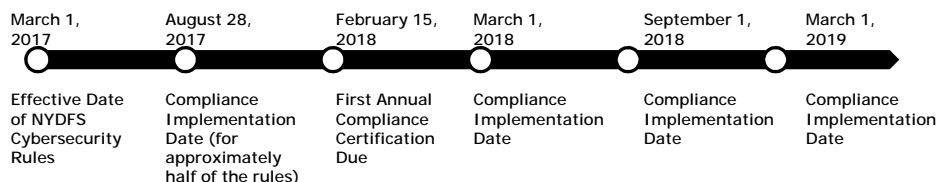
- For the purpose of seeking or providing legal advice
 - Aids in the careful evaluation of any threats/intrusions and responsive action for investigation, legal obligations, and litigation
 - Early in the process
 - Risks if not properly used/protected
- Company counsel working with outside counsel
- Role of counsel with vendors
 - At the direction of counsel

**Confidential Document
Attorney-Client Privilege**

Morgan Lewis

28

Phased-In Implementation



Morgan Lewis

29

Phased-In Implementation

- March 1, 2017 – Effective date of Rule; 180-day compliance implementation period for most of the Rule's requirements
- August 28, 2017 – General compliance implementation date
 - Cybersecurity program (500.2)
 - Cybersecurity policy (500.3)
 - Designation of CISO (500.4)
 - Limitations on access privileges (500.7)
 - Requirements for cybersecurity personnel and intelligence (500.10)
 - Incident response plan (500.16)
 - NYDFS notification requirements (500.17)
 - (Confidentiality protections) (500.18)
 - (Exemptions) (500.19)
 - NYDFS enforcement (500.20)

Morgan Lewis

[Section 500.22]

30

Phased-In Implementation

- February 15, 2018 – First annual compliance certification due
- March 1, 2018 – Compliance implementation date for:
 - CISO annual report to board of directors (500.4(b))
 - Penetration testing and vulnerability assessment (500.5)
 - Risk assessment (500.9)
 - Multi-factor authentication (500.12)
 - Cybersecurity awareness training for employees (500.14(b))

Morgan Lewis

[Section 500.22]

31

Phased-In Implementation

- September 1, 2018 – Compliance implementation date for:
 - Audit trail (500.6)
 - Application security (500.8)
 - Data retention limitations (500.13)
 - Authorized user monitoring requirements (500.14(a))
 - Encryption of nonpublic information (500.15)
- March 1, 2019 – Compliance implementation date for third-party service provider (TPSP) security policy (500.11)

Morgan Lewis

[Section 500.22]

32

Cybersecurity Program

- Foundational requirement of the cybersecurity rule
- Overall requirement: the cybersecurity program must “protect the confidentiality, integrity and availability of the Covered Entity’s Information Systems”
- Must be based on required risk assessment (500.09)
- Must do the following:
 - Identify and assess internal and external cybersecurity risks that may threaten the security or integrity of Nonpublic Information
 - Use defensive infrastructure and policies/procedures to protect Information Systems and stored Nonpublic Information from unauthorized access and malicious acts
 - Detect, respond to and recover from Cybersecurity Events
 - Comply with applicable regulatory reporting requirements

Morgan Lewis

[Section 500.02]

33

Cybersecurity Program

- Reliance on affiliates
 - Permitted, if the affiliate’s cybersecurity program is compliant with the NYDFS rule as applicable to the Covered Entity
- NYDFS must have full access to all cybersecurity program documentation

Morgan Lewis

[Section 500.02]

34

Cybersecurity Policy

- Written procedures, guidelines and standards
- Must be approved by the board of directors or equivalent governing body
 - Board of directors committee may approve
- Must consist of policies and procedures to protect
 - Information Systems
 - Nonpublic information
- Must be based on the required risk assessment

Morgan Lewis

[Section 500.03]

35

Cybersecurity Policy

- 14 required elements of the Cybersecurity Policy
 - information security
 - data governance and classification
 - asset inventory and device management
 - access controls and identity management
 - business continuity and disaster recovery planning and resources
 - systems operations and availability concerns
 - systems and network security
 - systems and network monitoring
 - systems and application development and quality assurance
 - physical security and environmental controls
 - customer data privacy
 - vendor and Third Party Service Provider management
 - risk assessment
 - incident response

Morgan Lewis

[Section 500.03]

36

Risk Assessment

- Another foundational requirement of the cybersecurity rule
- General requirement is for a “periodic” risk assessment of covered entity information systems. In turn, the risk assessment will provide a framework for the required cybersecurity policy.
- Required risk assessment must be performed in accordance with “written policies and procedures” that specify how:
 - cybersecurity risks or threats will be evaluated and categorized
 - the “confidentiality, integrity, security and availability” of covered information will be assessed
 - identified risks will be mitigated or accepted, and how the cybersecurity program will address these risks
- “Periodic” updating is required

Morgan Lewis

[Section 500.09]

37

Chief Information Security Officer (CISO)

- Core CISO requirements
 - Qualified person
 - Responsible for cybersecurity program implementation, oversight and enforcement
 - CISO reporting obligation: annual (or more frequent) report to board of directors or senior officer responsible for cybersecurity program
- Some conditional flexibility in the designation process
 - CISO may be employed by the covered entity, an affiliate, or a TPSP
 - The covered entity cannot outsource its responsibility to comply with the regulations
 - If employed by a TPSP, a senior covered entity official must oversee the TPSP, and the TPSP must maintain a cybersecurity program that protects the covered entity

Morgan Lewis

[Section 500.04]

38

Chief Information Security Officer (CISO)

- Annual report elements:
 - Confidentiality of nonpublic information
 - Integrity and security of information systems
 - Cybersecurity policies and procedures
 - “Material” cybersecurity risks
 - Overall effectiveness of cybersecurity program
 - Material Cybersecurity Events during the reporting period
- Compliance considerations
 - CISO is a functional position, not a required title
 - The level of CISO qualifications required is not fixed; it will be a function of the covered entity's size, business profile and risk profile
 - CISO obligations are specified and defined in the NYDFS regulations as a whole, not just this one section
 - CISO designation comes with some liability attached

Morgan Lewis

[Section 500.04]

39

New Notification Requirement



(a) Notice of Cybersecurity Event. Each Covered Entity shall notify the superintendent as promptly as possible but in no event later than 72 hours from a determination that a Cybersecurity Event has occurred that is either of the following:

- (1) Cybersecurity Events impacting the Covered Entity of which notice is required to be provided to any government body, self-regulatory agency or any other supervisory body; or
- (2) Cybersecurity Events that have a reasonable likelihood of materially harming any material part of the normal operation(s) of the Covered Entity.

Morgan Lewis

[Section 500.17(a)]

40

New Notification Requirement



(a) Notice of Cybersecurity Event. Each Covered Entity shall notify the superintendent as promptly as possible but in no event later than **72 hours** from a determination that a **Cybersecurity Event** has occurred that is either of the following:

- (1) Cybersecurity Events impacting the Covered Entity of which notice is required to be provided to any government body, self-regulatory agency or any other supervisory body; or
- (2) Cybersecurity Events that have a reasonable likelihood of materially harming any material part of the normal operation(s) of the Covered Entity.

Morgan Lewis

[Section 500.17(a)]

41

New Notification Requirement



(a) Notice of Cybersecurity Event. Each Covered Entity shall notify the superintendent as promptly as possible but in no event later than 72 hours from a determination that a Cybersecurity Event has occurred that is either of the following:

- (1) Cybersecurity Events impacting the Covered Entity of which **notice is required** to be provided **to any government body, self-regulatory agency or any other supervisory body**; or
- (2) Cybersecurity Events that have a reasonable likelihood of materially harming any material part of the normal operation(s) of the Covered Entity.

Morgan Lewis

[Section 500.17(a)]

42

New Notification Requirement



(a) Notice of Cybersecurity Event. Each Covered Entity shall notify the superintendent as promptly as possible but in no event later than 72 hours from a determination that a Cybersecurity Event has occurred that is either of the following:

(1) Cybersecurity Events impacting the Covered Entity of which notice is required to be provided to any government body, self-regulatory agency or any other supervisory body; or

(2) **Cybersecurity Events** that have a **reasonable likelihood of materially harming any material part of the normal operation(s)** of the Covered Entity.

Morgan Lewis

[Section 500.17(a)]

43

New Notification Requirement



(a) Notice of Cybersecurity Event. Each Covered Entity shall notify the superintendent as promptly as possible but in no event later than 72 hours from a determination that a Cybersecurity Event has occurred that is either of the following:

(1) Cybersecurity Events impacting the Covered Entity of which notice is required to be provided to any government body, self-regulatory agency or any other supervisory body; or

(2) **Cybersecurity Events** that have a **reasonable likelihood of materially harming any material part of the normal operation(s)** of the Covered Entity.

Morgan Lewis

[Section 500.17(a)]

44

Annual Compliance Certification



- Annual Certification Requirement
 - February 15, 2018

- “[C]ertifying that the Covered Entity is in compliance with the requirements set forth in this Part.”

APPENDIX A (Part 500)

(Covered Entity Name) _____

February 15, 20____

Certification of Compliance with New York State Department of Financial Services Cybersecurity Regulations

The Board of Directors or a Senior Officer(s) of the Covered Entity certifies:

(1) The Board of Directors (or name of Senior Officer(s)) has reviewed documents, reports, certifications and opinions of such officers, employees, representatives, outside vendors and other individuals or entities as necessary;

(2) To the best of the (Board of Directors) or (name of Senior Officer(s)) knowledge, the Cybersecurity Program of (name of Covered Entity) as of _____ (date of the Board Resolution or Senior Officer(s) Compliance Finding) for the year ended _____ (year for which Board Resolution or Compliance Finding is provided) complies with Part _____.

Signed by the Chairperson of the Board of Directors or Senior Officer(s)

(Name) _____ Date: _____

[DFS Portal Filing Instructions]

Morgan Lewis

[Section 500.17(b)]

45

Annual Compliance Certification



- Record Keeping Requirement
 - Maintain for DFS examination “all records, schedules and data supporting this certificate”
 - 5 years

- Remedial Efforts Identified
 - For “material improvement, updating or redesign” areas
 - “[D]ocument the identification and the remedial efforts planned and underway to address such areas, systems or processes”
 - Records “available for inspection by the superintendent”

APPENDIX A (Part 500)

(Covered Entity Name) _____

February 15, 20____

Certification of Compliance with New York State Department of Financial Services Cybersecurity Regulations

The Board of Directors or a Senior Officer(s) of the Covered Entity certifies:

(1) The Board of Directors (or name of Senior Officer(s)) has reviewed documents, reports, certifications and opinions of such officers, employees, representatives, outside vendors and other individuals or entities as necessary;

(2) To the best of the (Board of Directors) or (name of Senior Officer(s)) knowledge, the Cybersecurity Program of (name of Covered Entity) as of _____ (date of the Board Resolution or Senior Officer(s) Compliance Finding) for the year ended _____ (year for which Board Resolution or Compliance Finding is provided) complies with Part _____.

Signed by the Chairperson of the Board of Directors or Senior Officer(s)

(Name) _____ Date: _____

[DFS Portal Filing Instructions]

Morgan Lewis

[Section 500.17(b)]

46

Third-Party Vendor Relationships

- Covered Entity may use TPSPs and other vendors to meet the requirements of the regulations.
- “Third Party Service Provider” is defined as a Person that (i) is not an Affiliate of the Covered Entity, (ii) provides services to the Covered Entity, and (iii) maintains, processes or otherwise is permitted access to Nonpublic Information through its provision of services to the Covered Entity.
- CISO and qualified cybersecurity personnel can be TPSP employees under the direction and oversight of the Covered Entity.

Morgan Lewis

[Section 500.11]

47

Third-Party Vendor Relationships

- A Covered Entity's cybersecurity policy should address TPSP management, including policies and procedures designed to ensure the security of Information Systems and Nonpublic Information that are accessible to or held by TPSPs.
- Identification and risk assessment of TPSPs, minimum required cybersecurity practices, due diligence processes to evaluate the adequacy of cybersecurity practices, and periodic assessments

Morgan Lewis

[Section 500.11]

48

Third-Party Vendor Relationships

- Due diligence of TPSPs should include evaluation of the TPSPs' policies and procedures for:
 - Access controls and use of Multi-Factor Authentication
 - Use of encryption to protect Nonpublic Information
- Contracts with TPSPs should include the following protections:
 - Notice to Covered Entity of a Cybersecurity Event directly impacting the Covered Entity's Information Systems or Nonpublic Information
 - Representations and warranties addressing the TPSPs' cybersecurity policies and procedures that are related to the security of the Covered Entity's Information Systems or Nonpublic Information

Morgan Lewis

[Section 500.11]

49

Incident Response Plan

- Written incident response plan should be designed to promptly respond to, and recover from, any Cybersecurity Event "materially affecting the confidentiality, integrity or availability of the Covered Entity's Information Systems or the continuing functionality of any aspect of the Covered Entity's business or operations."



Morgan Lewis

[Section 500.16]

50

Incident Response Plan

- Incident response plan should address:
 - Internal processes for responding to a Cybersecurity Event
 - The goals of the incident response plan
 - The definition of clear roles, responsibilities and levels of decision-making authority
 - External and internal communications and information sharing
 - Identification of requirements for the remediation of any identified weaknesses in Information Systems and associated controls
 - Documentation and reporting regarding Cybersecurity Events and related incident response activities
 - The evaluation and revision as necessary of the incident response plan following a Cybersecurity Event

Morgan Lewis

[Section 500.16]

51

Protection of Nonpublic Information

- “Nonpublic Information” is defined to include certain consumer information, individual health information, and business-related information of the Covered Entity.
- Various requirements for safeguarding and disposing of Nonpublic Information

**TOP
SECRET**

Morgan Lewis

[Sections 500.01, 07, 12]

52

Protection of Nonpublic Information

- Access controls
 - Access privileges to information systems that provide access to Nonpublic Information to be limited.
 - Effective controls to protect against unauthorized access to Nonpublic Information may include Multi-Factor Authentication
 - Multi-Factor Authentication is required for access to a Covered Entity's internal networks from an external network
- Encryption
 - Encryption and other controls to use implemented to protect Nonpublic Information held or transmitted by the Covered Entity both in transit over external networks and at rest.
 - Can use effective alternative compensating controls as reviewed and approved by the CISO

Morgan Lewis

[Sections 500.08, 13, 15]

53

Protection of Nonpublic Information

- Data Retention and Disposal
 - Periodic disposal of Nonpublic Information that is no longer necessary for business operations or other legitimate businesses purposes and is not otherwise required to be retained by law or regulation
- Application Security
 - Policies to include procedures to ensure secure development practices for in-house applications and for evaluating, assessing or testing the security of externally-developed applications

Morgan Lewis

[Sections 500.08, 13, 15]

54

Periodic Testing, Monitoring & Review

- Penetration Testing and Vulnerability Assessments
 - Goal of both is to assess the overall effectiveness of the cybersecurity program
 - Covered Entities can implement continuous monitoring or annual Penetration Testing and bi-annual vulnerability assessments
- Other specified periodic reviews:
 - Any encryption compensation controls to be reviewed annually by the CISO
 - Application security to be periodically reviewed by the CISO or its designee
 - Access privileges to be periodically reviewed by Covered Entity
 - Periodic assessment of TPSPs

Morgan Lewis

[Sections 500.05, 15]

55

Qualified Personnel & Training

DFS establishes rules related to “cybersecurity personnel” and all personnel.

1. Cybersecurity Personnel

- A Covered Entity must have qualified cybersecurity personnel (employed by the Covered Entity, an Affiliate or a TPSP) who are responsible for managing cybersecurity risks and performing or overseeing core cybersecurity functions.
- Cybersecurity personnel must be provided with cybersecurity updates and trained to address relevant cybersecurity risks.
- A Covered Entity must verify that key cybersecurity personnel are current regarding changes on cybersecurity threats and countermeasures.

Morgan Lewis

[Sections 500.10, 14]

56

Qualified Personnel & Training

2. All Personnel

- DFS categorizes personnel as Authorized Users when such personnel participate in a Covered Entity's business operations and are authorized to access and use the Covered Entity's Information Systems and data.
- A Covered Entity must maintain risk-based policies, procedures and controls used to:
 - monitor Authorized Users' activity; and
 - detect unauthorized access or use of, or tampering with, Nonpublic Information by Authorized Users.
- A Covered Entity must provide regular cybersecurity awareness training to all personnel, updated to reflect risks identified in the Covered Entity's risk assessment.

Morgan Lewis

[Sections 500.10, 14]

57

Audit Trail



- The Audit Trail requirement is based on a Covered Entity's risk assessment and mandates that a Covered Entity securely maintain systems that:
 - Reconstruct material financial transactions sufficient to support normal operations and the Covered Entity's obligations.
 - A Covered Entity must maintain these records for **five years**.
 - Are designed to detect and respond to Cybersecurity Events that have a reasonable likelihood of materially harming any material part of the normal operations of the Covered Entity.
 - Note: DFS uses the same language here as it does in the notification requirement.
 - A Covered Entity must maintain these records for **three years**.

Morgan Lewis

[Section 500.06]

58

Audit Trail



- The final Audit Trail requirements are less burdensome than the originally proposed requirements, providing more flexibility to Covered Entities.
- DFS no longer requires:
 - A six-year recordkeeping requirement
 - Logs of physical access to the Audit Trail hardware and protection of the integrity of hardware from alterations or tampering
 - Records of access and alterations made to Audit Trail systems

Morgan Lewis

[Section 500.06]

59

Liability for Noncompliance

- The rules include an enforcement provision, which states:

This regulation will be enforced by the superintendent pursuant to, and is not intended to limit, the superintendent's authority under any applicable laws.
- DFS is not shy about taking enforcement action against firms it regulates. Earlier this year, DFS and a foreign bank entered into a consent order whereby the foreign bank agreed to pay \$425 million for the failure to maintain an effective and compliant AML program.
- It remains unclear whether the annual compliance certificate could present legal liability to those who sign the certificate or whether DFS will fine Covered Entities or otherwise impose penalties for noncompliance.
- It is also unclear how DFS intends to use audit trail records, and if DFS will inspect audit trail records after the occurrence of a Cybersecurity Event.

Morgan Lewis

[Section 500.20]

60

NY STATE DEPARTMENT OF FINANCIAL SERVICES CYBERSECURITY RULE

PRACTICAL CONSIDERATIONS

Practical Considerations

- Need to think about any and all operations in NY
- Who will serve as the CISO?
- What third-party relationships need to be evaluated?
- Does the rule cover insurance agents in NY?
- How does the rule apply to foreign bank branches whose cybersecurity functions are implemented and controlled from the home office?
- How does a board get comfortable signing the certification?

Morgan Lewis

62

NY STATE DEPARTMENT OF FINANCIAL SERVICES CYBERSECURITY RULE

RESPONDING TO A "CYBERSECURITY EVENT"

Some Preliminary Questions

- Did a "Cybersecurity Event" occur?
 - Contrast "data breach"
- When was the cyber incident discovered?
 - How was the cyber incident discovered?
- How did the cyber incident occur?
- When did the cyber incident occur?
 - Early assessments can be revised
- Who caused the cyber compromise/incident?
 - Attribution analysis
- What are the risks?

Morgan Lewis

64

Overseeing an Internal Investigation

- Determine scope and nature of breach or “Cybersecurity Event”
 - Note: Different triggering standards used by different enforcers
 - Roller coaster of ups and downs
- Attorney client privilege
 - Is the privilege effectively in place?
- Assess legal consequences
 - What regulatory agencies?
 - Was information accessed, acquired, or exfiltrated?
 - Which customers?
 - What legal standards apply?



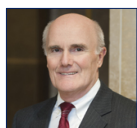
Morgan Lewis

65

NY STATE DEPARTMENT OF FINANCIAL SERVICES CYBERSECURITY RULE

Q&A

Questions



Charles Horn
Morgan Lewis
Washington, DC
Telephone 202.739.5951
charles.horn@morganlewis.com



Mark Krotoski
Morgan Lewis
Silicon Valley, California
Washington, DC
Telephone 650.843.7212
Telephone 202.739.5024
mark.krotoski@morganlewis.com



Melissa Hall
Morgan Lewis
Washington, D.C.
Telephone 202.739.5883
melissa.hall@morganlewis.com



Sarah Riddell
Morgan Lewis
Chicago
Telephone 312.324.1154
sarah.riddell@morganlewis.com

Morgan Lewis

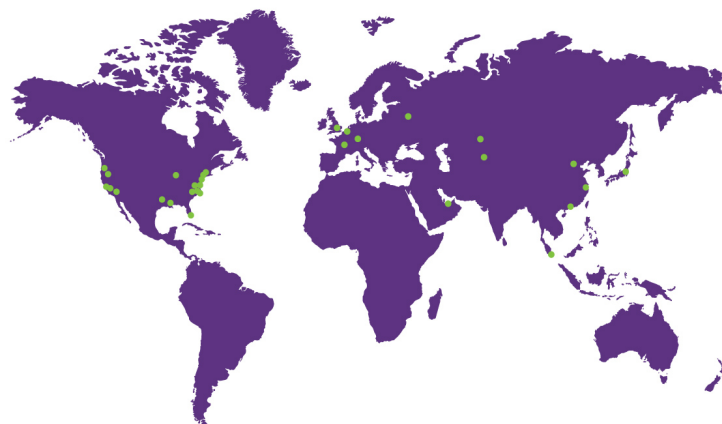
67

Our Global Reach

Africa
Asia Pacific
Europe
Latin America
Middle East
North America

Our Locations

Almaty	Dallas	London	Paris	Shanghai*
Astana	Dubai	Los Angeles	Philadelphia	Silicon Valley
Beijing*	Frankfurt	Miami	Pittsburgh	Singapore
Boston	Hartford	Moscow	Princeton	Tokyo
Brussels	Hong Kong*	New York	San Francisco	Washington, DC
Chicago	Houston	Orange County	Santa Monica	Wilmington



Morgan Lewis

*Our Beijing office operates as a representative office of Morgan, Lewis & Bockius LLP. In Shanghai, we operate as a branch of Morgan Lewis Consulting (Beijing) Company Limited, and an application to establish a representative office of the firm is pending before the Ministry of Justice. In Hong Kong, Morgan Lewis has filed an application to become a registered foreign law firm and is seeking approval with The Law Society of Hong Kong to associate with Luk & Partners.

THANK YOU

© 2017 Morgan, Lewis & Bockius LLP
© 2017 Morgan Lewis Stamford LLC
© 2017 Morgan, Lewis & Bockius UK LLP

Morgan, Lewis & Bockius UK LLP is a limited liability partnership registered in England and Wales under number OC378797 and is a law firm authorised and regulated by the Solicitors Regulation Authority. The SRA authorisation number is 615176.

*Our Beijing office operates as a representative office of Morgan, Lewis & Bockius LLP. In Shanghai, we operate as a branch of Morgan Lewis Consulting (Beijing) Company Limited, and an application to establish a representative office of the firm is pending before the Ministry of Justice. In Hong Kong, Morgan Lewis has filed an application to become a registered foreign law firm and is seeking approval with The Law Society of Hong Kong to associate with Luk & Partners. This material is provided for your convenience and does not constitute legal advice or create an attorney-client relationship. Prior results do not guarantee similar outcomes. Attorney Advertising.

Morgan Lewis

69

**NEW YORK STATE
DEPARTMENT OF FINANCIAL SERVICES
23 NYCRR 500**

CYBERSECURITY REQUIREMENTS FOR FINANCIAL SERVICES COMPANIES

I, Maria T. Vullo, Superintendent of Financial Services, pursuant to the authority granted by sections 102, 201, 202, 301, 302 and 408 of the Financial Services Law, do hereby promulgate Part 500 of Title 23 of the Official Compilation of Codes, Rules and Regulations of the State of New York, to take effect March 1, 2017, to read as follows:

(ALL MATTER IS NEW)

Section 500.00 Introduction.

The New York State Department of Financial Services (“DFS”) has been closely monitoring the ever-growing threat posed to information and financial systems by nation-states, terrorist organizations and independent criminal actors. Recently, cybercriminals have sought to exploit technological vulnerabilities to gain access to sensitive electronic data. Cybercriminals can cause significant financial losses for DFS regulated entities as well as for New York consumers whose private information may be revealed and/or stolen for illicit purposes. The financial services industry is a significant target of cybersecurity threats. DFS appreciates that many firms have proactively increased their cybersecurity programs with great success.

Given the seriousness of the issue and the risk to all regulated entities, certain regulatory minimum standards are warranted, while not being overly prescriptive so that cybersecurity programs can match the relevant risks and keep pace with technological advances. Accordingly, this regulation is designed to promote the protection of customer information as well as the information technology systems of regulated entities. This regulation requires each company to assess its specific risk profile and design a program that addresses its risks in a robust fashion. Senior management must take this issue seriously and be responsible for the organization’s cybersecurity program and file an annual certification confirming compliance with these regulations. A regulated entity’s cybersecurity program must ensure the safety and soundness of the institution and protect its customers.

It is critical for all regulated institutions that have not yet done so to move swiftly and urgently to adopt a cybersecurity program and for all regulated entities to be subject to minimum standards with respect to their programs. The number of cyber events has been steadily increasing and estimates of potential risk to our financial services industry are stark. Adoption of the program outlined in these regulations is a priority for New York State.

Section 500.01 Definitions.

For purposes of this Part only, the following definitions shall apply:

(a) *Affiliate* means any Person that controls, is controlled by or is under common control with another Person. For purposes of this subsection, control means the possession, direct or indirect, of the power to direct or cause the direction of the management and policies of a Person, whether through the ownership of stock of such Person or otherwise.

(b) *Authorized User* means any employee, contractor, agent or other Person that participates in the business operations of a Covered Entity and is authorized to access and use any Information Systems and data of the Covered Entity.

(c) *Covered Entity* means any Person operating under or required to operate under a license, registration, charter, certificate, permit, accreditation or similar authorization under the Banking Law, the Insurance Law or the Financial Services Law.

(d) *Cybersecurity Event* means any act or attempt, successful or unsuccessful, to gain unauthorized access to, disrupt or misuse an Information System or information stored on such Information System.

(e) *Information System* means a discrete set of electronic information resources organized for the collection, processing, maintenance, use, sharing, dissemination or disposition of electronic information, as well as any specialized system such as industrial/process controls systems, telephone switching and private branch exchange systems, and environmental control systems.

(f) *Multi-Factor Authentication* means authentication through verification of at least two of the following types of authentication factors:

- (1) Knowledge factors, such as a password; or
- (2) Possession factors, such as a token or text message on a mobile phone; or
- (3) Inherence factors, such as a biometric characteristic.

(g) *Nonpublic Information* shall mean all electronic information that is not Publicly Available Information and is:

(1) Business related information of a Covered Entity the tampering with which, or unauthorized disclosure, access or use of which, would cause a material adverse impact to the business, operations or security of the Covered Entity;

(2) Any information concerning an individual which because of name, number, personal mark, or other identifier can be used to identify such individual, in combination with any one or more of the following data elements: (i) social security number, (ii) drivers' license number or non-driver identification card number, (iii) account number, credit or debit card number, (iv) any security code, access code or password that would permit access to an individual's financial account, or (v) biometric records;

(3) Any information or data, except age or gender, in any form or medium created by or derived from a health care provider or an individual and that relates to (i) the past, present or future physical, mental or behavioral health or condition of any individual or a member of the individual's family, (ii) the provision of health care to any individual, or (iii) payment for the provision of health care to any individual.

(h) *Penetration Testing* means a test methodology in which assessors attempt to circumvent or defeat the security features of an Information System by attempting penetration of databases or controls from outside or inside the Covered Entity's Information Systems.

(i) *Person* means any individual or any non-governmental entity, including but not limited to any non-governmental partnership, corporation, branch, agency or association.

(j) *Publicly Available Information* means any information that a Covered Entity has a reasonable basis to believe is lawfully made available to the general public from: federal, state or local government records; widely distributed media; or disclosures to the general public that are required to be made by federal, state or local law.

(1) For the purposes of this subsection, a Covered Entity has a reasonable basis to believe that information is lawfully made available to the general public if the Covered Entity has taken steps to determine:

(i) That the information is of the type that is available to the general public; and

(ii) Whether an individual can direct that the information not be made available to the general public and, if so, that such individual has not done so.

(k) *Risk Assessment* means the risk assessment that each Covered Entity is required to conduct under section 500.09 of this Part.

(l) *Risk-Based Authentication* means any risk-based system of authentication that detects anomalies or changes in the normal use patterns of a Person and requires additional verification of the Person's identity when such deviations or changes are detected, such as through the use of challenge questions.

(m) *Senior Officer(s)* means the senior individual or individuals (acting collectively or as a committee) responsible for the management, operations, security, information systems, compliance and/or risk of a Covered Entity, including a branch or agency of a foreign banking organization subject to this Part.

(n) *Third Party Service Provider(s)* means a Person that (i) is not an Affiliate of the Covered Entity, (ii) provides services to the Covered Entity, and (iii) maintains, processes or otherwise is permitted access to Nonpublic Information through its provision of services to the Covered Entity.

Section 500.02 Cybersecurity Program.

(a) *Cybersecurity Program*. Each Covered Entity shall maintain a cybersecurity program designed to protect the confidentiality, integrity and availability of the Covered Entity's Information Systems.

(b) The cybersecurity program shall be based on the Covered Entity's Risk Assessment and designed to perform the following core cybersecurity functions:

(1) identify and assess internal and external cybersecurity risks that may threaten the security or integrity of Nonpublic Information stored on the Covered Entity's Information Systems;

(2) use defensive infrastructure and the implementation of policies and procedures to protect the Covered Entity's Information Systems, and the Nonpublic Information stored on those Information Systems, from unauthorized access, use or other malicious acts;

(3) detect Cybersecurity Events;

(4) respond to identified or detected Cybersecurity Events to mitigate any negative effects;

(5) recover from Cybersecurity Events and restore normal operations and services; and

(6) fulfill applicable regulatory reporting obligations.

(c) A Covered Entity may meet the requirement(s) of this Part by adopting the relevant and applicable provisions of a cybersecurity program maintained by an Affiliate, provided that such provisions satisfy the requirements of this Part, as applicable to the Covered Entity.

(d) All documentation and information relevant to the Covered Entity's cybersecurity program shall be made available to the superintendent upon request.

Section 500.03 Cybersecurity Policy.

Cybersecurity Policy. Each Covered Entity shall implement and maintain a written policy or policies, approved by a Senior Officer or the Covered Entity's board of directors (or an appropriate committee thereof) or equivalent governing body, setting forth the Covered Entity's policies and procedures for the protection of its Information Systems and Nonpublic Information stored on those Information Systems. The cybersecurity policy shall be based on the Covered Entity's Risk Assessment and address the following areas to the extent applicable to the Covered Entity's operations:

(a) information security;

(b) data governance and classification;

(c) asset inventory and device management;

(d) access controls and identity management;

(e) business continuity and disaster recovery planning and resources;

(f) systems operations and availability concerns;

(g) systems and network security;

(h) systems and network monitoring;

(i) systems and application development and quality assurance;

- (j) physical security and environmental controls;
- (k) customer data privacy;
- (l) vendor and Third Party Service Provider management;
- (m) risk assessment; and
- (n) incident response.

Section 500.04 Chief Information Security Officer.

(a) Chief Information Security Officer. Each Covered Entity shall designate a qualified individual responsible for overseeing and implementing the Covered Entity's cybersecurity program and enforcing its cybersecurity policy (for purposes of this Part, "Chief Information Security Officer" or "CISO"). The CISO may be employed by the Covered Entity, one of its Affiliates or a Third Party Service Provider. To the extent this requirement is met using a Third Party Service Provider or an Affiliate, the Covered Entity shall:

- (1) retain responsibility for compliance with this Part;
- (2) designate a senior member of the Covered Entity's personnel responsible for direction and oversight of the Third Party Service Provider; and
- (3) require the Third Party Service Provider to maintain a cybersecurity program that protects the Covered Entity in accordance with the requirements of this Part.

(b) Report. The CISO of each Covered Entity shall report in writing at least annually to the Covered Entity's board of directors or equivalent governing body. If no such board of directors or equivalent governing body exists, such report shall be timely presented to a Senior Officer of the Covered Entity responsible for the Covered Entity's cybersecurity program. The CISO shall report on the Covered Entity's cybersecurity program and material cybersecurity risks. The CISO shall consider to the extent applicable:

- (1) the confidentiality of Nonpublic Information and the integrity and security of the Covered Entity's Information Systems;
- (2) the Covered Entity's cybersecurity policies and procedures;
- (3) material cybersecurity risks to the Covered Entity;
- (4) overall effectiveness of the Covered Entity's cybersecurity program; and
- (5) material Cybersecurity Events involving the Covered Entity during the time period addressed by the report.

Section 500.05 Penetration Testing and Vulnerability Assessments.

The cybersecurity program for each Covered Entity shall include monitoring and testing, developed in accordance with the Covered Entity's Risk Assessment, designed to assess the effectiveness of the Covered Entity's cybersecurity program. The monitoring and testing shall include continuous monitoring or periodic Penetration Testing and vulnerability assessments. Absent effective continuous monitoring, or other systems to detect, on an ongoing basis, changes in Information Systems that may create or indicate vulnerabilities, Covered Entities shall conduct:

(a) annual Penetration Testing of the Covered Entity's Information Systems determined each given year based on relevant identified risks in accordance with the Risk Assessment; and

(b) bi-annual vulnerability assessments, including any systematic scans or reviews of Information Systems reasonably designed to identify publicly known cybersecurity vulnerabilities in the Covered Entity's Information Systems based on the Risk Assessment.

Section 500.06 Audit Trail.

(a) Each Covered Entity shall securely maintain systems that, to the extent applicable and based on its Risk Assessment:

(1) are designed to reconstruct material financial transactions sufficient to support normal operations and obligations of the Covered Entity; and

(2) include audit trails designed to detect and respond to Cybersecurity Events that have a reasonable likelihood of materially harming any material part of the normal operations of the Covered Entity.

(b) Each Covered Entity shall maintain records required by section 500.06(a)(1) of this Part for not fewer than five years and shall maintain records required by section 500.06(a)(2) of this Part for not fewer than three years.

Section 500.07 Access Privileges.

As part of its cybersecurity program, based on the Covered Entity's Risk Assessment each Covered Entity shall limit user access privileges to Information Systems that provide access to Nonpublic Information and shall periodically review such access privileges.

Section 500.08 Application Security.

(a) Each Covered Entity's cybersecurity program shall include written procedures, guidelines and standards designed to ensure the use of secure development practices for in-house developed applications utilized by the Covered Entity, and procedures for evaluating, assessing or testing the security of externally developed applications utilized by the Covered Entity within the context of the Covered Entity's technology environment.

(b) All such procedures, guidelines and standards shall be periodically reviewed, assessed and updated as necessary by the CISO (or a qualified designee) of the Covered Entity.

Section 500.09 Risk Assessment.

(a) Each Covered Entity shall conduct a periodic Risk Assessment of the Covered Entity's Information Systems sufficient to inform the design of the cybersecurity program as required by this Part. Such Risk Assessment shall be updated as reasonably necessary to address changes to the Covered Entity's Information Systems, Nonpublic Information or business operations. The Covered Entity's Risk Assessment shall allow for revision of controls to respond to technological developments and evolving threats and shall consider the particular risks of the Covered Entity's business operations related to cybersecurity, Nonpublic Information collected or stored, Information Systems utilized and the availability and effectiveness of controls to protect Nonpublic Information and Information Systems.

(b) The Risk Assessment shall be carried out in accordance with written policies and procedures and shall be documented. Such policies and procedures shall include:

(1) criteria for the evaluation and categorization of identified cybersecurity risks or threats facing the Covered Entity;

(2) criteria for the assessment of the confidentiality, integrity, security and availability of the Covered Entity's Information Systems and Nonpublic Information, including the adequacy of existing controls in the context of identified risks; and

(3) requirements describing how identified risks will be mitigated or accepted based on the Risk Assessment and how the cybersecurity program will address the risks.

Section 500.10 Cybersecurity Personnel and Intelligence.

(a) Cybersecurity Personnel and Intelligence. In addition to the requirements set forth in section 500.04(a) of this Part, each Covered Entity shall:

(1) utilize qualified cybersecurity personnel of the Covered Entity, an Affiliate or a Third Party Service Provider sufficient to manage the Covered Entity's cybersecurity risks and to perform or oversee the performance of the core cybersecurity functions specified in section 500.02(b)(1)-(6) of this Part;

(2) provide cybersecurity personnel with cybersecurity updates and training sufficient to address relevant cybersecurity risks; and

(3) verify that key cybersecurity personnel take steps to maintain current knowledge of changing cybersecurity threats and countermeasures.

(b) A Covered Entity may choose to utilize an Affiliate or qualified Third Party Service Provider to assist in complying with the requirements set forth in this Part, subject to the requirements set forth in section 500.11 of this Part.

Section 500.11 Third Party Service Provider Security Policy.

(a) Third Party Service Provider Policy. Each Covered Entity shall implement written policies and procedures designed to ensure the security of Information Systems and Nonpublic Information that are accessible

to, or held by, Third Party Service Providers. Such policies and procedures shall be based on the Risk Assessment of the Covered Entity and shall address to the extent applicable:

(1) the identification and risk assessment of Third Party Service Providers;

(2) minimum cybersecurity practices required to be met by such Third Party Service Providers in order for them to do business with the Covered Entity;

(3) due diligence processes used to evaluate the adequacy of cybersecurity practices of such Third Party Service Providers; and

(4) periodic assessment of such Third Party Service Providers based on the risk they present and the continued adequacy of their cybersecurity practices.

(b) Such policies and procedures shall include relevant guidelines for due diligence and/or contractual protections relating to Third Party Service Providers including to the extent applicable guidelines addressing:

(1) the Third Party Service Provider's policies and procedures for access controls, including its use of Multi-Factor Authentication as required by section 500.12 of this Part, to limit access to relevant Information Systems and Nonpublic Information;

(2) the Third Party Service Provider's policies and procedures for use of encryption as required by section 500.15 of this Part to protect Nonpublic Information in transit and at rest;

(3) notice to be provided to the Covered Entity in the event of a Cybersecurity Event directly impacting the Covered Entity's Information Systems or the Covered Entity's Nonpublic Information being held by the Third Party Service Provider; and

(4) representations and warranties addressing the Third Party Service Provider's cybersecurity policies and procedures that relate to the security of the Covered Entity's Information Systems or Nonpublic Information.

(c) Limited Exception. An agent, employee, representative or designee of a Covered Entity who is itself a Covered Entity need not develop its own Third Party Information Security Policy pursuant to this section if the agent, employee, representative or designee follows the policy of the Covered Entity that is required to comply with this Part.

Section 500.12 Multi-Factor Authentication.

(a) Multi-Factor Authentication. Based on its Risk Assessment, each Covered Entity shall use effective controls, which may include Multi-Factor Authentication or Risk-Based Authentication, to protect against unauthorized access to Nonpublic Information or Information Systems.

(b) Multi-Factor Authentication shall be utilized for any individual accessing the Covered Entity's internal networks from an external network, unless the Covered Entity's CISO has approved in writing the use of reasonably equivalent or more secure access controls.

Section 500.13 Limitations on Data Retention.

As part of its cybersecurity program, each Covered Entity shall include policies and procedures for the secure disposal on a periodic basis of any Nonpublic Information identified in section 500.01(g)(2)-(3) of this Part that is no longer necessary for business operations or for other legitimate business purposes of the Covered Entity, except where such information is otherwise required to be retained by law or regulation, or where targeted disposal is not reasonably feasible due to the manner in which the information is maintained.

Section 500.14 Training and Monitoring.

As part of its cybersecurity program, each Covered Entity shall:

(a) implement risk-based policies, procedures and controls designed to monitor the activity of Authorized Users and detect unauthorized access or use of, or tampering with, Nonpublic Information by such Authorized Users; and

(b) provide regular cybersecurity awareness training for all personnel that is updated to reflect risks identified by the Covered Entity in its Risk Assessment.

Section 500.15 Encryption of Nonpublic Information.

(a) As part of its cybersecurity program, based on its Risk Assessment, each Covered Entity shall implement controls, including encryption, to protect Nonpublic Information held or transmitted by the Covered Entity both in transit over external networks and at rest.

(1) To the extent a Covered Entity determines that encryption of Nonpublic Information in transit over external networks is infeasible, the Covered Entity may instead secure such Nonpublic Information using effective alternative compensating controls reviewed and approved by the Covered Entity's CISO.

(2) To the extent a Covered Entity determines that encryption of Nonpublic Information at rest is infeasible, the Covered Entity may instead secure such Nonpublic Information using effective alternative compensating controls reviewed and approved by the Covered Entity's CISO.

(b) To the extent that a Covered Entity is utilizing compensating controls under (a) above, the feasibility of encryption and effectiveness of the compensating controls shall be reviewed by the CISO at least annually.

Section 500.16 Incident Response Plan.

(a) As part of its cybersecurity program, each Covered Entity shall establish a written incident response plan designed to promptly respond to, and recover from, any Cybersecurity Event materially affecting the confidentiality, integrity or availability of the Covered Entity's Information Systems or the continuing functionality of any aspect of the Covered Entity's business or operations.

(b) Such incident response plan shall address the following areas:

(1) the internal processes for responding to a Cybersecurity Event;

- (2) the goals of the incident response plan;
- (3) the definition of clear roles, responsibilities and levels of decision-making authority;
- (4) external and internal communications and information sharing;
- (5) identification of requirements for the remediation of any identified weaknesses in Information Systems and associated controls;
- (6) documentation and reporting regarding Cybersecurity Events and related incident response activities; and
- (7) the evaluation and revision as necessary of the incident response plan following a Cybersecurity Event.

Section 500.17 Notices to Superintendent.

(a) Notice of Cybersecurity Event. Each Covered Entity shall notify the superintendent as promptly as possible but in no event later than 72 hours from a determination that a Cybersecurity Event has occurred that is either of the following:

- (1) Cybersecurity Events impacting the Covered Entity of which notice is required to be provided to any government body, self-regulatory agency or any other supervisory body; or
- (2) Cybersecurity Events that have a reasonable likelihood of materially harming any material part of the normal operation(s) of the Covered Entity.

(b) Annually each Covered Entity shall submit to the superintendent a written statement covering the prior calendar year. This statement shall be submitted by February 15 in such form set forth as Appendix A, certifying that the Covered Entity is in compliance with the requirements set forth in this Part. Each Covered Entity shall maintain for examination by the Department all records, schedules and data supporting this certificate for a period of five years. To the extent a Covered Entity has identified areas, systems or processes that require material improvement, updating or redesign, the Covered Entity shall document the identification and the remedial efforts planned and underway to address such areas, systems or processes. Such documentation must be available for inspection by the superintendent.

Section 500.18 Confidentiality.

Information provided by a Covered Entity pursuant to this Part is subject to exemptions from disclosure under the Banking Law, Insurance Law, Financial Services Law, Public Officers Law or any other applicable state or federal law.

Section 500.19 Exemptions.

- (a) Limited Exemption. Each Covered Entity with:

(1) fewer than 10 employees, including any independent contractors, of the Covered Entity or its Affiliates located in New York or responsible for business of the Covered Entity, or

(2) less than \$5,000,000 in gross annual revenue in each of the last three fiscal years from New York business operations of the Covered Entity and its Affiliates, or

(3) less than \$10,000,000 in year-end total assets, calculated in accordance with generally accepted accounting principles, including assets of all Affiliates,

shall be exempt from the requirements of sections 500.04, 500.05, 500.06, 500.08, 500.10, 500.12, 500.14, 500.15, and 500.16 of this Part.

(b) An employee, agent, representative or designee of a Covered Entity, who is itself a Covered Entity, is exempt from this Part and need not develop its own cybersecurity program to the extent that the employee, agent, representative or designee is covered by the cybersecurity program of the Covered Entity.

(c) A Covered Entity that does not directly or indirectly operate, maintain, utilize or control any Information Systems, and that does not, and is not required to, directly or indirectly control, own, access, generate, receive or possess Nonpublic Information shall be exempt from the requirements of sections 500.02, 500.03, 500.04, 500.05, 500.06, 500.07, 500.08, 500.10, 500.12, 500.14, 500.15, and 500.16 of this Part.

(d) A Covered Entity under Article 70 of the Insurance Law that does not and is not required to directly or indirectly control, own, access, generate, receive or possess Nonpublic Information other than information relating to its corporate parent company (or Affiliates) shall be exempt from the requirements of sections 500.02, 500.03, 500.04, 500.05, 500.06, 500.07, 500.08, 500.10, 500.12, 500.14, 500.15, and 500.16 of this Part.

(e) A Covered Entity that qualifies for any of the above exemptions pursuant to this section shall file a Notice of Exemption in the form set forth as Appendix B within 30 days of the determination that the Covered Entity is exempt.

(f) The following Persons are exempt from the requirements of this Part, provided such Persons do not otherwise qualify as a Covered Entity for purposes of this Part: Persons subject to Insurance Law section 1110; Persons subject to Insurance Law section 5904; and any accredited reinsurer or certified reinsurer that has been accredited or certified pursuant to 11 NYCRR 125.

(g) In the event that a Covered Entity, as of its most recent fiscal year end, ceases to qualify for an exemption, such Covered Entity shall have 180 days from such fiscal year end to comply with all applicable requirements of this Part.

Section 500.20 Enforcement.

This regulation will be enforced by the superintendent pursuant to, and is not intended to limit, the superintendent's authority under any applicable laws.

Section 500.21 Effective Date.

This Part will be effective March 1, 2017. Covered Entities will be required to annually prepare and submit to the superintendent a Certification of Compliance with New York State Department of Financial Services Cybersecurity Regulations under section 500.17(b) of this Part commencing February 15, 2018.

Section 500.22 Transitional Periods.

(a) Transitional Period. Covered Entities shall have 180 days from the effective date of this Part to comply with the requirements set forth in this Part, except as otherwise specified.

(b) The following provisions shall include additional transitional periods. Covered Entities shall have:

(1) One year from the effective date of this Part to comply with the requirements of sections 500.04(b), 500.05, 500.09, 500.12, and 500.14(b) of this Part.

(2) Eighteen months from the effective date of this Part to comply with the requirements of sections 500.06, 500.08, 500.13, 500.14 (a) and 500.15 of this Part.

(3) Two years from the effective date of this Part to comply with the requirements of section 500.11 of this Part.

Section 500.23 Severability.

If any provision of this Part or the application thereof to any Person or circumstance is adjudged invalid by a court of competent jurisdiction, such judgment shall not affect or impair the validity of the other provisions of this Part or the application thereof to other Persons or circumstances.

APPENDIX A (Part 500)

(Covered Entity Name)

February 15, 20____

Certification of Compliance with New York State Department of Financial Services Cybersecurity Regulations

The Board of Directors or a Senior Officer(s) of the Covered Entity certifies:

(1) The Board of Directors (or name of Senior Officer(s)) has reviewed documents, reports, certifications and opinions of such officers, employees, representatives, outside vendors and other individuals or entities as necessary;

(2) To the best of the (Board of Directors) or (name of Senior Officer(s)) knowledge, the Cybersecurity Program of (name of Covered Entity) as of_____(date of the Board Resolution or Senior Officer(s) Compliance Finding) for the year ended__(year for which Board Resolution or Compliance Finding is provided) complies with Part ____.

Signed by the Chairperson of the Board of Directors or Senior Officer(s)

(Name)_____

Date: _____

[DFS Portal Filing Instructions]

APPENDIX B (Part 500)

(Covered Entity Name)

(Date)_____

Notice of Exemption

In accordance with 23 NYCRR § 500.19(e), (Covered Entity Name) hereby provides notice that (Covered Entity Name) qualifies for the following Exemption(s) under 23 NYCRR § 500.19 (check all that apply):

- ☐ Section 500.19(a)(1)
- ☐ Section 500.19(a)(2)
- ☐ Section 500.19(a)(3)
- ☐ Section 500.19(b)
- ☐ Section 500.19(c)
- ☐ Section 500.19(d)

If you have any question or concerns regarding this notice, please contact:

(Insert name, title, and full contact information)

(Name)_____

Date: _____

(Title)

(Covered Entity Name)

[DFS Portal Filing Instructions]

DATA BREACH CHECKLIST

PHASE I: ALERT AND ORGANIZATION

1. Company alerted to possible data breach—record date, time, and method of alert
2. Notify internal Incident Response Team (IRT), consisting of a representative from
 - a. Information Technology
 - b. Legal/Compliance
 - c. Outside Counsel (Morgan Lewis)
 - d. HR
 - e. Public Relations
 - f. Customer Service
 - g. Executive
3. Identify an Incident Lead for this incident – performs as project manager
4. Contact outside counsel at Morgan Lewis
5. Convene conference call of IRT
6. Consider hiring forensic technology partner depending on available internal resources and complexity of breach
7. Notify insurance carrier/understand scope of preauthorization or limitations on third-party vendor reimbursement
8. Check with counsel on proper role and implementation of the attorney-client privilege in the data breach investigation

PHASE II: INITIAL SCOPING BEFORE CONTAINING AN ONGOING BREACH

1. Identify, document, and preserve scope of compromise to the extent possible within 24–48 hours
2. Consider notifications or steps to take before stopping the breach that may prevent harm in the event the act of stopping the breach alerts data thieves that you have discovered them
3. Preserve any evidence related to the ongoing breach

PHASE III: CONTAIN THE BREACH

1. Be sure that the full scope of compromise is understood to the extent possible within 24–48 hours
2. Contain/arrest the breach—stop any possible flow of data to unauthorized recipients
3. Document results of containment effort

PHASE IV: INVESTIGATION

1. Root cause analysis
2. Classify type of breach
 - a. Hacking
 - b. Internal
 - c. Loss/Theft of Tangible Data (computer, device, storage media)
 - d. Inadvertent Disclosure
 - e. Loss with No Known Disclosure
 - f. Other
3. Full identification of data compromised
 - a. Type of information compromised
 - i. Sensitive personal information
 1. Social Security numbers
 2. Credit card information
 3. Financial account data
 4. Medical information
 5. Usernames and passwords
 6. Driver's license numbers
 7. Other sensitive personal information (disclosure of which could cause harm)
 - ii. Other personal information
 1. Contact information (name, address, email address, phone number, etc.)
 2. Preferences, purchase history
 3. Other information linked to a person that is not sensitive
 - b. Individuals whose information was compromised, including where they reside

4. Determine nature of any unauthorized recipients
 - a. Employee acquisition in good faith
 - b. Business partner
 - c. Trustworthy recipient who normally receives information of this nature
 - d. Unknown individuals, but definite disclosure
 - e. Lost information—may not have been disclosed
 - f. Suspected bad actor/employee not in good faith
 - g. Known bad actor/departed or departing employee
5. Assess known or discoverable actual use of compromised information
6. Undertake security updates necessary before notification

PHASE V: NOTIFICATIONS (IN LIGHT OF INFORMATION DEVELOPED IN PHASE IV)

1. Before notifications
 - a. Develop PR plan for potential media inquiries
 - b. Consider notification to company board of directors or others who should be notified before public
 - c. Prepare for inquiries from affected individuals—call center or other
2. If criminal and depending on seriousness and other factors, notify law enforcement—local, FBI, Secret Service, or other
3. If required by law or recommended because individuals could do something to prevent further harm to themselves, make notifications to affected individuals. If made,
 - a. Include what happened, what the company has done, and what the individual can do to prevent any harm
 - b. Include legally required information and resources available from government agencies
 - c. Consider an offer of identity theft prevention/credit monitoring depending on nature of information compromised
4. Notifications to government agencies and Attorneys General as required by law
5. Other notifications as required by information at issue
6. Evaluate feedback from notifications and determine if additional steps/notifications are required

PHASE VI: POST-NOTIFICATIONS

1. Disclosures to investors, stockholders, SEC, securities disclosures, etc.
2. Cost recoveries—responsible third parties, insurance, other
3. Consider longer-term security upgrades or other measures to prevent reoccurrence or similar events
4. Analyze data breach notification plan/checklist for necessary changes in light of lessons learned
5. Prepare final reports
 - a. Executive report with a summary of what happened, how it was addressed, what notifications were provided, and steps taken to prevent future incidents of the same or similar nature
 - b. Technical report with detailed background of the event; evidentiary backup for analysis, decisions, and conclusions; and evidence of preventative measures

REMINDERS

- Maintain confidentiality—update IRT and executives frequently; other disclosures only to those who need to know
 - Preserve evidence and information for future investigations
 - Document events with dates and times; record reasons for determinations made
-

HOW WE CAN HELP

If we can be of assistance to you regarding your data collection, maintenance, protection, or suspected breach, contact a Morgan Lewis lawyer listed below:

Reece Hirsch | San Francisco
+1.415.442.1422 | rhirsch@morganlewis.com

Mark L. Krotoski | Silicon Valley
+1.650.843.7212 | mkrotoski@morganlewis.com

Gregory T. Parks | Philadelphia
+1.215.963.5170 | gparks@morganlewis.com

Reproduced with permission from Privacy & Security Law Report, 15 PVLR 271, 2/8/16. Copyright © 2016 by The Bureau of National Affairs, Inc. (800-372-1033) <http://www.bna.com>

Data Breach Notification

Companies will be left in a legal quagmire of inconsistent state data breach notification requirements unless Congress repairs the broken system by passing legislation to replace the patchwork of state laws, the authors write, as they analyze proposals for implementing a unified federal standard.

The Need to Repair the Complex, Cumbersome, Costly Data Breach Notification Maze



BY MARK L. KROTOSKI, LUCY WANG, AND JENNIFER S. ROSEN

Mark L. Krotoski is a litigation partner in the Privacy and Cybersecurity and Antitrust practices of Morgan, Lewis & Bockius LLP in Silicon Valley and Washington. He previously served as the National Coordinator of the Computer Hacking and Intellectual Property Program in the Criminal Division of the U.S. Department of Justice.

Lucy Wang is an associate in the Litigation practice of Morgan, Lewis & Bockius in San Francisco.

Jennifer S. Rosen is an associate in the Litigation practice of Morgan, Lewis & Bockius in San Francisco.

I. Introduction

Companies face many cyber-threats from several sources today. Significant data breaches can result from organized, international hacking groups; state-sponsored actors; hackers for hire; cyber terrorists; hacktivists; an insider threat; and even employee inadvertence or misconduct. The perpetrators seek information of value ranging from social security numbers, health information, credit card numbers and confidential company information to trade secrets. Much of the time, however, the data breach is a result of cyber-crime.

After a breach, a number of data breach notifications are triggered for customers and also enforcement agencies. In fact, navigating the notification requirements can become a cumbersome nightmare. The failure to do so properly can result in lawsuits and enforcement actions.

Consider a common recent data breach example: Sophisticated cyber-thieves launch a spearfishing e-mail attack against a target company. Despite cyber-trainings and policies, the company discovers that an employee's e-mail account was compromised.¹ Consequently, the criminals penetrated the company's security systems, accessed and stole confidential information.

Upon discovery, the company immediately launched an investigation to determine the cause and scope of the breach. For example, did the hackers access personally identifiable information (PII), protected health information (PHI), payment card information (PCI), trade secrets or other confidential information? Moreover, were any customers impacted and what if any information was exfiltrated or used? The answers may take weeks to determine. The full scope of the breach may not be known for several months.

After being the victim of a cybercrime, however, the company must also confront a maze of disclosure obligations. The customer notification requirements will depend on the customer's residence and jurisdiction of enforcement agencies. Almost every state has data breach notification requirements, but they can differ significantly in their scope and application. In California and Florida, for example, a customer's user name and security question would qualify as protected information. Not so in Wisconsin or Connecticut. State laws differ not only in the types of data breaches they regulate, but also in who, what, when and how they require companies to notify their customers. In California, Florida and Connecticut, for example, companies may also be required to notify particular state agencies. Hence, even though the company operates nationally and its security systems are managed centrally, the company must tailor each notification to fit the specific requirements of the state in which each customer resides.

The variations between each state's laws create a complex and burdensome system for companies operating across many jurisdictions.

Failure to do so exposes the company to state penalties for technical non-compliance as well as potential civil litigation. Depending on the type of information (e.g., PII, PHI, PCI or trade secrets), companies may be subject to multiple overlapping federal and state regimes. For example, reporting may be required to the Securities and Exchange Commission (SEC),² Dep't of

Health and Human Serv. (HHS),³ Federal Communication Commission (FCC),⁴ and other federal and state agencies. Again, some states, including California and Wisconsin, exempt companies from their data notification laws if the subject information is separately regulated under a the Health Insurance Portability and Accountability Act (HIPAA). Other states, such as Florida and Connecticut, have no such exemption.

Consider, for example, the issue of "who" must be notified. Data breach standards differ on whether the customer or individual must be notified every time there is a breach. Some states—such as Connecticut, Florida, and Wisconsin⁵—have a harm analysis that is used to determine whether notification is required, while others—such as California⁶—do not.

In addition to notifying the individual, some state laws require a public report filing but differ on the circumstances when the report must be filed. Illustratively, California and Florida require a report when the PII was disclosed for more than 500 residents.⁷ When notice is given to more than 1,000 persons, other states require notice such as Hawaii which requires notification to the Office of Consumer Protection,⁸ Missouri requiring notice to "the attorney general's office and all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis,"⁹ and North Carolina similarly requiring notice to "the Consumer Protection Division of the Attorney General's Office and all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis."¹⁰ Massachusetts requires notification of the breach to the "to the attorney general, the director of consumer affairs and business regulation and to such [affected] resident."¹¹ Under these different state statutes, the same breach incident can result in mandated disclosures to individuals and public agencies in some jurisdictions but not others. With state data breach notification laws becoming increasingly complex and often conflicting, the objective of assisting consumers has become unnecessarily complex, costly and cumbersome. The question now is whether this multitude of state laws is creating more confusion than clarity and undermining the original objectives for data breach notification? The notification process should not be this challenging for compliance.

This article analyzes the development of state notification laws and current proposals for implementing a unified federal standard. For the reasons discussed below, policymakers should act to simply the notification requirements so they remain meaningful.

³ See, e.g., HIPAA Breach Notification Rule, 45 CFR § § 164.400-414; see also Notice to the Sec'y of HHS, Breach of Unsecured Protected Health Information.

⁴ See, e.g., 47 C.F.R. 64.2011 (Notification of customer proprietary network information security breaches); see also Customer Proprietary Network Information (CPNI) Breach Reporting Facility.

⁵ See Conn. Gen. Stat. § 36a-701b; Fla. Stat. § § 501.171, 282.0041, 282.318(2)(i); Wis. Stat. § 134.98.

⁶ See Cal. Civ. Code § § 1798.29(*), 1798.80(*).

⁷ Cal. Civ. Code § § 1798.29(e), 1798.80(f); Fla. Stat. § § 501.171, 282.0041, 282.318(2)(i).

⁸ Haw. Rev. Stat. § § 487N-2(f).

⁹ Mo. Rev. Stat. § 407.1500.2(8).

¹⁰ N.C. Gen. Stat. § § 75-61, 75-65(f).

¹¹ Mass. Gen. Laws § 93H-1.3(b).

¹ The example draws upon the recent "Business E-mail Compromise" which has adversely impacted many financial services and other companies. See, e.g., U.S. Dep't of Justice, Fed. Bureau of Investigation, Fin. Serv. Info. Sharing and Analysis Ctr. and U.S. Secret Serv., *Fraud Alert—Business E-mail Compromise Continues to Swindle and Defraud U.S. Businesses* (June 19, 2015), <http://src.bna.com/cge>.

² See, e.g., Div. of Corp. Fin., Sec. and Exch. Comm'n, CF Disclosure Guidance: Topic No. 2, Cybersecurity (Oct. 13, 2011).

II. Proliferating State Data Breach Notification Laws

In 2002, California enacted the first data security breach notification law, which became effective in July 2003.¹² The objective of this new law was to allow consumers to protect themselves against identity theft and mitigate damages resulting from unauthorized access to their information.¹³ In a little more than a decade, the state data breach standards have proliferated. Today, 47 states, the District of Columbia, Guam, Puerto Rico and the U.S. Virgin Islands have adopted data breach notification laws.¹⁴

Broadly speaking, most data breach notification laws follow the basic tenets of California's original law. In each jurisdiction, lawmakers passed laws requiring entities to notify individuals when there is a reasonable belief of unauthorized acquisition of or access to data that compromises the security, confidentiality or integrity of an individual's covered personal information.¹⁵ Responding to a data breach under any of these laws, however, is a multi-step process—a company must (1) ascertain if a breach has occurred; (2) determine whether the data at issue (typically PII) triggers data breach notification in one or more of the 51 applicable jurisdictions (in addition to any federal notification requirements); (3) determine who to notify (such as customers and public agencies); and (4) determine what, when, and how to notify them.¹⁶

a. Conflicts Between State Notification Laws.

Based on the proliferation of data breach notification standards, compliance with data breach notification laws can be complicated in any one jurisdiction, and the variations between each state's laws create a complex and burdensome system for companies operating across many jurisdictions. Companies operating in each of the 51 jurisdictions must, for example, must identify and reconcile the differences between requirements such as the timing of the notification. While some state's notification laws require quicker notification than others', in practice, multi-jurisdictional companies must determine, and uniformly follow, the most rigorous applicable standard in order to streamline the process. This requires familiarity with each of the differing notification windows, some of which are defined vaguely as the "most expedient time possible,"¹⁷ and others which range from as few as 30 days,¹⁸ to as many as 90 days.¹⁹

Once a business has identified the shortest applicable notification period, it must wade through the many other differences between data breach notification laws. Most immediately, it is necessary to determine what kind of PII is covered under the applicable states'

laws. While most states' definitions of PII cover similar ground—social security number, driver's license number, state ID card number and account or credit/debit card number along with an access code²⁰—some states have expanded definitions of protected PII subject to the data breach notification laws, such as a user name/e-mail address and password²¹, and an individual's DNA profile or unique biometric data (e.g., fingerprint, voice print, retina or iris image).²² Even where states' definitions of PII overlap, there are often nuanced distinctions that make a significant impact on an entity's notification obligations. For instance, some states protect only *electronic* data,²³ while others protect PII in any form.²⁴

Making the discovery and notification process even more cumbersome, states' notification triggers vary from an unauthorized "acquisition" of PII,²⁵ to unauthorized "access" to PII,²⁶ and in some states either an unauthorized acquisition or unauthorized access can trigger the notification laws.²⁷ Moreover, some states provide exemptions from the notification laws where an entity has complied with separate laws. For example, some (but not all) states exempt entities that are covered by HIPAA and have complied with the notice requirements in Section 13402(f) of the Health Information Technology for Economic and Clinical Health Act (HITECH).²⁸

A comparison of a few sample states' requirements further demonstrates the complicated maze of the state data breach notification laws:

b. Evolving New Standards and Moving Targets.

To complicate matters, because the laws in this area are constantly evolving, the most rigorous standards across each applicable jurisdiction are moving targets. For instance, in 2015, at least 32 states introduced or are considering, security breach notification bills or resolutions.³³ Among other things, these bills contemplate amending existing data breach notification laws to require entities to report breaches to the local attorney general or another central state agency; expand the definition of PII (e.g., to include medical, insurance or biometric data); require businesses or government entities to implement security plans or various security measures; and require educational institutions to notify parents or government entities if a breach occurs.³⁴ California alone enacted several laws this year amending its data breach notification requirements.³⁵ Among other things, the new laws include data collected through the use of an automated license plate recogni-

²⁰ See, e.g., Cal. Civ. Code § § 1798.29, 1798.82; Conn. Gen. Stat. § 36a-701b; Fla. Stat. § § 501.171, 282.0041, 282.318(2)(i); Wis. Stat. § 134.98.

²¹ See, e.g., Cal. Civ. Code § 1798.29(g)(2); Fla. Stat. § 501.171(g).

²² See, e.g., Wis. Stat. § 134.98(1)(b).

²³ See, e.g., Cal. Civ. Code § 1798.29(a); Fla. Stat. § 501.171(1)(a); Conn. Gen. Stat. § 36a-701b(a).

²⁴ See, e.g., Wis. Stat. § 134.98.

²⁵ See, e.g., Cal. Civ. Code § 1798.29(f); Wis. Stat. § 134.98.

²⁶ See, e.g., Fla. Stat. § 501.171(1)(a).

²⁷ See, e.g., Conn. Gen. Stat. § 36a-701b(a).

²⁸ See, e.g., Cal. Civ. Code § 1798.81.5(e)(3); Wis. Stat. § 134.98(3m)(b).

³³ NCSL, 2015 Security Breach Legislation.

³⁴ *Id.*

³⁵ *Id.*

¹² S.B. 1386 (Cal. 2002) (amending Cal. Civ. Code § § 1798.29, 1798.82).

¹³ *Id.* at § 1.

¹⁴ See Nat'l Conference of State Legislatures (NCSL), Security Breach Notification Laws (listing jurisdictions).

¹⁵ See, e.g., Conn. Gen. Stat. § 36a-701b; Fla. Stat. § § 501.171, 282.0041, 282.318(2)(i); Wis. Stat. § 134.98.

¹⁶ *Id.*

¹⁷ See, e.g., Cal. Civ. Code § 1798.29(a).

¹⁸ See, e.g., Fla. Stat. § 501.171(4)(a).

¹⁹ See, e.g., S.B. 949 (Conn. 2015) (amending Conn. Gen. Stat. § 36a-701b).

Data Breach Notification Maze

California ^[1]	Florida ^[2]	Wisconsin ^[3]	Connecticut ^[4]
Definition of Personally Identifying Information (PII)			
<p>(1) An individual's first name or first initial and last name in combination with:</p> <ul style="list-style-type: none"> • Social Security Number; • Driver license number; • State ID card number; • Account number or credit card / debit card number in connection with any code permitting access to an individual's financial account; • Medical information; • Health insurance information <p>Or</p> <p>(2) User name or email address, in combination with a password or security question and answer that would permit access to an online account.</p>	<p>(1) An individual's first name or first initial and last name in combination with:</p> <ul style="list-style-type: none"> • Social Security Number; • Driver license number; • State ID card number; • Account number or credit card/debit card number in connection with any code permitting access to an individual's financial account; • Medical information; • Health insurance information • Passport number; • Military ID number; • Any other number issued on a government document used to verify identity; <p>Or</p> <p>(2) User name or email address, in combination with a password or security question and answer that would permit access to an online account.</p>	<p>An individual's first and last name or first initial and last name in combination with:</p> <ul style="list-style-type: none"> • Social Security Number; • Driver license number; • State ID card number; • Account number or credit card/debit card number in connection with any code permitting access to an individual's financial account; • DNA profile; • Unique biometric data, including fingerprint, voice print, retina or iris image, or any other unique physical representation. 	<p>An individual's first name or first initial and last name in combination with:</p> <ul style="list-style-type: none"> • Social Security Number; • Driver license number; • State ID card number • Account number or credit/debit card number with any required code permitting access to an individual's financial account.
Notification Trigger			
When an Entity discovers or is notified of an unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of PII maintained by the Entity.	When an Entity knows, or reasonably believes, there has been unauthorized access to PII in electronic form.	When an Entity discovers or is notified that PII in the Entity's possession has been acquired by a person whom the Entity has not authorized to acquire the PII.	When an Entity knows, or reasonably believes, there has been unauthorized access to or acquisition of electronic files, media, databases, or computerized data containing PII.
Timing of Notification			
The most expedient time possible without unreasonable delay.	30 days	45 days	90 days
Attorney General to be Notified?			
Yes (if an Entity is required to notify more than 500 CA residents).	Yes (if an Entity is required to notify more than 500 individuals in FL).	No.	Yes.
<p>^[1] Cal. Civ. Code §§ 1798.29, 1798.80 et seq. ^[2] Fla. Stat. §§ 501.171, 282.0041, 282.318(2)(i). ^[3] Wis. Stat. § 134.98. ^[4] Conn. Gen Stat. § 36a-701b.</p>			
A BNA Graphic/data29g1			

Data Breach Notification Maze

California ^[1]	Florida ^[2]	Wisconsin ^[3]	Connecticut ^[4]
Manner of Notification			
<p>The notice shall disclose any breach of the security of the system following discovery or notification of the breach.</p> <p>Notice may be provided by:</p> <ul style="list-style-type: none"> • Mail; or • Electronically, provided it is consistent with 15 U.S.C. § 7001 (E-SIGN Act). • The notice shall be written in plain language and shall include (among other things) a description of: <ul style="list-style-type: none"> • The date of the notice; • Name and contact information of the Entity; • Type of PII subject to the unauthorized access and acquisition; • The date, estimated date, or date range during which the breach occurred; • Whether notification was delayed as a result of law enforcement investigation; • A general description of the breach incident; • The toll-free telephone numbers and addresses of the major credit reporting agencies if the breach exposed a social security number or a driver's license or California identification card number. 	<p>Attorney General Written notice must include (among other things):</p> <ul style="list-style-type: none"> • A synopsis of the events surrounding the breach • The number of individuals in Florida who were or have potentially been affected by the breach. • A copy of the notice required to affected individuals. <p>Affected Individuals Notice must contain, at a minimum:</p> <ul style="list-style-type: none"> • The date, estimated date, or estimated date range of the breach. • A description of the PII that was accessed or reasonably believed to have been accessed. • Information regarding how to contact the Entity to inquire about the breach. <p>Notice may be provided by:</p> <ul style="list-style-type: none"> • Mail; or • E-mail. 	<p>The notice shall indicate that the Entity knows of the unauthorized acquisition of PII.</p> <p>Notice may be provided by:</p> <ul style="list-style-type: none"> • Mail; or • A method the Entity has previously employed to communicate with the subject of the PII. 	<p>The notice shall disclose any breach of security following the discovery of the breach.</p> <p>Notice may be provided by:</p> <ul style="list-style-type: none"> • Mail; • Telephone; or • Electronically, provided it is consistent with 15 U.S.C. § 7001 (E-SIGN Act). • Additionally, Entities must offer and disclose identity theft prevention services and, if applicable, identity theft mitigation services, at no cost for up to one year.
Risk of Harm Exemption			
No.	Yes—notice to affected individuals is not required if the Entity reasonably determines that the breach has not and will not likely result in identity theft or any other financial harm to those whose PII has been accessed.	Yes—an Entity is not required to provide notice of the acquisition of PII if the acquisition of PII does not create a material risk of identity theft or fraud to the subject of the PII.	Yes—notification is not required if the Entity reasonably determines that the breach will not likely result in harm to those whose PII has been acquired and accessed.
HIPPA Exception			
Yes.	No.	Yes.	No.
<p>^[1] Cal. Civ. Code §§ 1798.29, 1798.80 et seq. ^[2] Fla. Stat. §§ 501.171, 282.0041, 282.318(2)(i). ^[3] Wis. Stat. § 134.98. ^[4] Conn. Gen Stat. § 36a-701b.</p>			

tion system within the scope of protected PII.³⁶ This marks the third set of amendments to California's notification laws within the last three years.³⁷

c. The Effects of Disparate State Notification Laws.

The patchwork of state laws related to data security make corporate compliance with the notification laws both unnecessarily difficult and costly. Moreover, even after conducting a comprehensive investigation and response to the breach itself, there is still the risk that companies may face litigation for non-compliance with some technical requirements of each state's notification laws. According to a study conducted by the Ponemon Institute in May 2015, the average cost of a data breach to a U.S. company in 2015 was \$6.5 million, which represents an 11% increase in the total cost of data breach since 2014.³⁸

Such burdens and costs often do not result in the protections the laws are intended to provide. With such a confusing system of requirements, consumers are left without confidence in the safeguards protecting their personal information. According to a 2012 study by the Ponemon Institute, 72% of people who receive notification of a data breach were dissatisfied with the communication they received.³⁹

The consequences of non-compliance can result in enforcement actions by state attorneys general or other agencies.⁴⁰ Additionally, some states (such as California, Hawaii and Louisiana) permit a private right of action to be brought for the failure to provide timely disclosure.⁴¹

³⁶ *Id.*

³⁷ LawFlash, California Amends its Breach Notification Requirements (AGAIN) (Nov. 19, 2015) (summarizing new California data breach requirements) (14 PVLR 1893, 10/19/15).

³⁸ Ponemon Institute, 2015 Cost of Data Breach Study: United States.

³⁹ Ponemon Institute, 2012 Consumer Study on Data Breach Notification.

⁴⁰ Many state data breach statute provide for state enforcement actions. *See, e.g.*, Ariz. Rev. Stat. § 44-7501H ("This section may only be enforced by the attorney general. The attorney general may bring an action to obtain actual damages for a wilful and knowing violation of this section and a civil penalty not to exceed ten thousand dollars per breach of the security of the system or series of breaches of a similar nature that are discovered in a single investigation."); Kan. Stat. § 50-7a02(g) ("For violations of this section, except as to insurance companies licensed to do business in this state, the attorney general is empowered to bring an action in law or equity to address violations of this section and for other relief that may be appropriate.").

⁴¹ *See, e.g.*, Cal. Civ. Code § 1798.84(b) ("Any customer injured by a violation of this title may

institute a civil action to recover damages."); Haw. Rev. Stat. § 487N-3(b) ("any business that violates any provision of this chapter shall be liable to the injured party in an amount equal to the sum of any actual damages sustained by the injured party as a result of the violation"); La. Rev. Stat. § 51:3075 ("A civil action may be instituted to recover actual damages resulting from the failure to disclose in a timely manner to a person that there has been a breach of the security system resulting in the disclosure of a person's personal information.").

III. Early Recognition on the Need for A Uniform Federal Standard

Within a couple of years of the first state laws going into effect, Congress was already considering multiple proposals for federal legislation. Indeed, the states themselves were calling for national leadership. In a letter to congressional leaders in 2005, Attorneys General from 48 states urged Congress to take action and create federal requirements for notifying consumers of data breaches. Attorneys General from states that had already passed notification laws as well as states without such laws agreed that consumers would benefit from a "national security breach notification law."⁴² Moreover, while the Attorneys General recommended that federal preemption should be limited in scope, they acknowledged that federal law may govern the "timing, manner and content of security breach notification laws."⁴³

In the decade that followed, every single Congress has considered—but failed to pass—a national security breach notification law. In that time, however, the need for federal legislation has only intensified. Not only have the instances of cyberattacks risen, but the proliferation of state notification laws have made it increasingly difficult for companies to deliver timely and consistent information to consumers.

IV. Competing National Standard Proposals

During his State of the Union Address, President Obama noted the importance of addressing cyber security issues and enacting legislation "to better meet the evolving threat of cyber attacks, combat identity theft, and protect our children's information."⁴⁴ One part of the Administration package included a Personal Data Notification & Protection Act.⁴⁵ If passed, the Personal Data Notification & Protection Act would replace the current patchwork of state laws with a unified national standard for notifying consumers when their personal information has been compromised.⁴⁶

The Personal Data Notification & Protection Act, however, is only one of many proposals currently pending before Congress. Like the mosaic of state laws, each federal proposal takes a slightly different position on what constitutes personal information, what conditions trigger notification, what information must be disclosed, when the information must be disclosed, and what consequences should be imposed for non-compliance. In addition, the federal proposals also differ on whether (or to what extent) federal law should preempt overlapping state laws.

Among the competing proposals, one gained early traction—the Data Security and Breach Notification Act

⁴² Testimony of Assistant Attorney General Julie Brill before Subcommittee on Financial Institutions and Consumer Credit Committee on Financial Services, U.S. House of Representatives (Nov. 9, 2005), enclosing Letter from Attorneys General to Congressional Leaders (Oct. 27, 2005; updated Nov. 7, 2005).

⁴³ *Id.*

⁴⁴ *Id.*

⁴⁵ The Personal Data Notification & Protection Act.

⁴⁶ The White House Office of the Press Secretary, Securing Cyberspace - Preside Obama Announces New Cybersecurity Legislative Proposal and other Cybersecurity Efforts (January 13, 2015).

(H.R. 1770).⁴⁷ Jointly authored by Representative Marsha Blackburn (R-Tenn.) and Representative Peter Welch (D-Vt.), the Data Security and Breach Notification Act focuses on the pressing concerns of identity theft and financial fraud in e-commerce. In that context, the act defines personal information to include social security numbers, financial and other account credentials (including biometric credentials) and names coupled with driver's license numbers.⁴⁸ Upon discovering a security breach impacting personal information, companies must conduct a good faith investigation and take necessary measures to determine the scope of the breach and restore the reasonable integrity, security and confidentiality of the data system.⁴⁹ Once the company has done so, it must notify consumers of the breach within 30 days unless there is no reasonable risk of identity theft, economic loss, economic harm or financial fraud.⁵⁰

States continue to enact new privacy laws and revise existing laws at an almost feverish pace, which may, individually, be in the best interest of each states' residents. Taken collectively, however, this mish-mash of constantly changing state law is making it increasingly difficult for companies keep consumers informed.

Under the legislation, companies may delay notification for law enforcement or national security purposes.⁵¹ Otherwise, however, failure to notify constitutes an unfair and deceptive act or practice under the Federal Trade Commission Act.⁵² Both the FTC and State Attorneys General have enforcement power to seek civil penalties from violators.⁵³

Finally, consistent with the President's proposal, Data Security and Breach Notification Act would also create a unified national standard by preempting state notification laws.⁵⁴

V. Opposition from State Attorneys General

Just as the Data Security and Breach Notification Act is gaining some momentum, however, State Attorneys General issued another letter, this time to block a national notification law. In a new letter to Congressional leaders this summer, Attorneys General from forty seven states joined in opposing any federal legislation that would preclude states from enacting different or

more stringent requirements.⁵⁵ Attorneys General from several states—including California, Massachusetts and Illinois—have also spoken out individually, sometimes specifically to criticize the Data Security and Breach Notification Act.⁵⁶

Among other things, the State Attorneys General argue that Data Security and Breach Notification Act and similar proposals undercut existing protections for consumers under state law.⁵⁷ Federal law, they argue, may set a national floor of protection. However, Congress should not prevent any State from enacting tougher laws within their borders nor restrict a State Attorney General's authority to pursue violators.

Echoing these concerns, a coalition of Democratic Senators and Representatives introduced a competing proposal—the Consumer Privacy Protection Act (S. 1158/H.R. 2977).⁵⁸ Unlike the Data Security and Breach Notification Act, the Consumer Privacy Protection Act only preempts state laws to the extent they contain “less stringent” requirements for notification.⁵⁹ Hence, the Consumer Privacy Protection Act allows State Attorneys General to continue enforcement actions under more restrictive state standards.

Federal preemption would not eliminate the role of state attorneys general. To the contrary, each of the federal legislative proposals contemplates that state attorneys generals will be able to bring enforcement actions for violations of the federal data breach notification law.

Meanwhile, the Data Security and Breach Notification Act itself has stalled. Although the bill passed through the House Energy and Commerce Committee in April, the vote was split along party lines: 29 (Republican) - 20 (Democrat).⁶⁰ Even the bill's original co-author, Democratic Representative Peter Welch, ultimately voted with other Democrats in opposing his own bill.⁶¹

⁵⁵ Letter from Attorneys General to Congressional Leaders (July 7, 2015).

⁵⁶ See, e.g., Letter from California Attorney General Kamala D. Harris to Chairman and Ranking Member of House Committee on Energy and Commerce (May 4, 2015); Office of Massachusetts Attorney General Maura Healey, AG Healey Raises Concerns About Federal Bill That Would Weaken Data Breach Protections for Massachusetts Residents (March 18, 2015); Office of Illinois Attorney General Lisa Madigan, Madigan Testifies as Congress Considers Data Breach Notification Law (Feb. 5, 2015).

⁵⁷ Letter from Attorneys General to Congressional Leaders (July 7, 2015).

⁵⁸ S. 1158, 114th Cong., 1st Sess. (2015); H.R. 2977, 114th Cong., 1st Sess. (2015).

⁵⁹ *Id.* § 205.

⁶⁰ Energy & Commerce Committee, United States House of Representatives, Data Security Solution Moves Forward (April 15, 2015);

⁶¹ Elise Viebeck, *Controversial Data Breach Bill Pass House Committee*, The Hill (April 15, 2015).

⁴⁷ H.R. 1770, 114th Cong. 1st Sess. (2015).

⁴⁸ *Id.* § 5.10(A).

⁴⁹ *Id.* § 3(a).

⁵⁰ *Id.* §§ 3(a)(3) & 3(c).

⁵¹ *Id.* § 3(c).

⁵² *Id.* § 4(a).

⁵³ *Id.* §§ 4(a) & 4(b).

⁵⁴ *Id.* § 6(a).

At this point, it remains uncertain whether Data Security and Breach Notification Act or any other proposal for federal legislation will gain sufficient support to become law.

VI. Inconsistent Standards Persist

Against the congressional debate, States continue to enact new laws and revise existing laws at an almost feverish pace. Taken individually, each State may be acting in the best interest of its residents in trying to keep consumers informed. Taken collectively, however, this mish-mash of constantly changing state law is making it increasingly difficult for companies to do just that. Instead of providing greater protections for consumers, States are creating a legal quagmire that only ends up impeding companies' abilities to respond effectively to data breaches. Policymakers need to consider how consumers are served by the data breach notification confusion that persists under current law.

Some clarity needs to be restored to the data breach notification process. At this juncture, only Congress can do so.

Contrary to the positions taken by the State Attorneys General, federal law would not gut protections for consumers. To be sure, whichever legislative proposal is ultimately passed, it will likely be narrower than some existing state laws. However, federal law will cover jurisdictions that currently have no data breach notification laws and will also likely be broader than some existing state laws.

More importantly, federal law would create a uniform national standard that would benefit both consumers and companies. Consumers across the country would have a clearer understanding of what information is protected. Companies will also be better prepared to respond to a data breach. Instead of trying to comply with a multitude of sometimes conflicting laws—and risking sanctions for potential technical

noncompliance—companies can instead devote their resources to quickly investigating and remedying the data breach.

Moreover, federal preemption would not eliminate the role of state attorneys general. To the contrary, each of the federal legislative proposals contemplates that state attorneys general will be able to bring enforcement actions for violations of the federal data breach notification law. State attorneys general, therefore, would continue to be at the forefront of protecting their residents when cybercriminals attack.

At the end of the day, all stakeholders—federal and state, Democrats and Republicans, companies and consumers—have the same shared goal. If (and more likely when) a company is the target of cybercrime, we want the company to investigate the breach and inform consumers whose personal information has been compromised. A unified national standard would set clear and consistent expectations for what steps companies must take and what information consumers can expect to receive in the event of a data breach.

VII. Conclusion

The current data breach notification laws are no longer working effectively. The process has become unnecessarily complex, costly and cumbersome.

There is no consensus among the states to simply or improve the process. Consequently, only Congress can repair the system. Bi-partisan support is needed for federal legislation to replace the current patchwork of state laws governing data breach notification. Without federal action, companies will be left in this legal quagmire of inconsistent state notification requirements. The maze of state laws is making it increasingly difficult for companies to notify customers with clear and timely information. Congress should step in to improve data notification standards. One federal standard will best serve the needs of both companies and consumers.