+

The Draft Amendments: Upcoming Changes to NYDFS Cybersecurity Rules

Society of Insurance Financial Management
Holiday Conference
November 17, 2022

JohnsonLambert
cpas + consultants

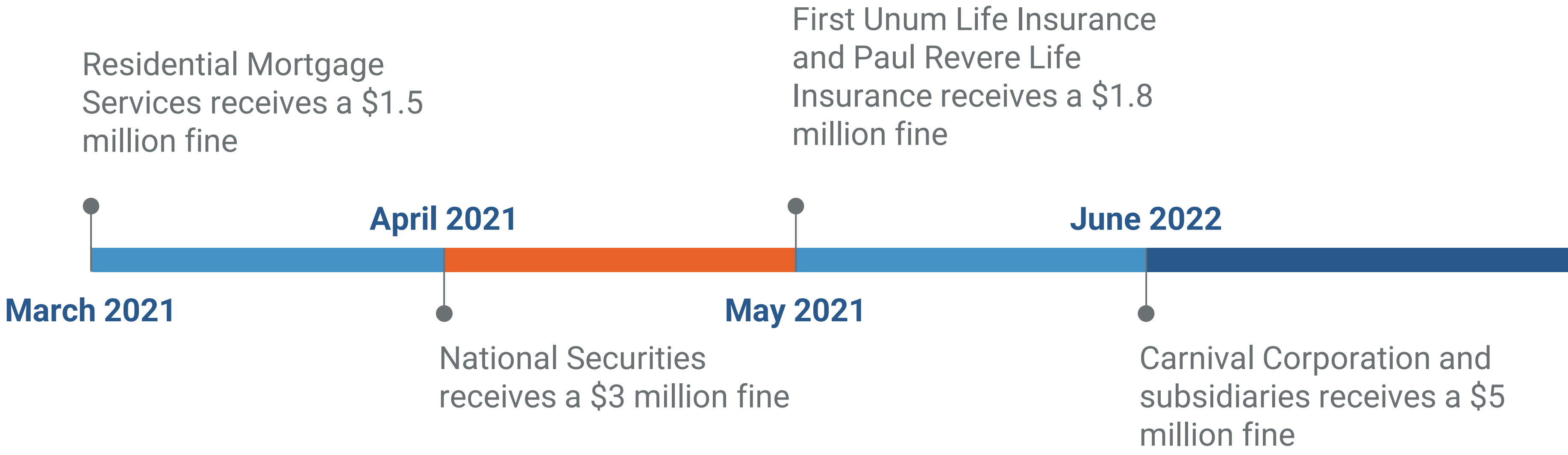
Agenda

- NYDFS Cyber Headlines
- Summary of Updates
    - New Type of Entity: Class A
    - Governance
    - Technology
    - Monitoring + Notification
    - Adoption Timeline
- FAQ + Takeaways

NYDFS Cyber Headlines

JohnsonLambert
cpas + consultants

Timeline of Events



March 2021

Residential Mortgage Services receives a $1.5 million fine

April 2021

National Securities receives a $3 million fine

May 2021

First Unum Life Insurance and Paul Revere Life Insurance receives a $1.8 million fine

June 2022

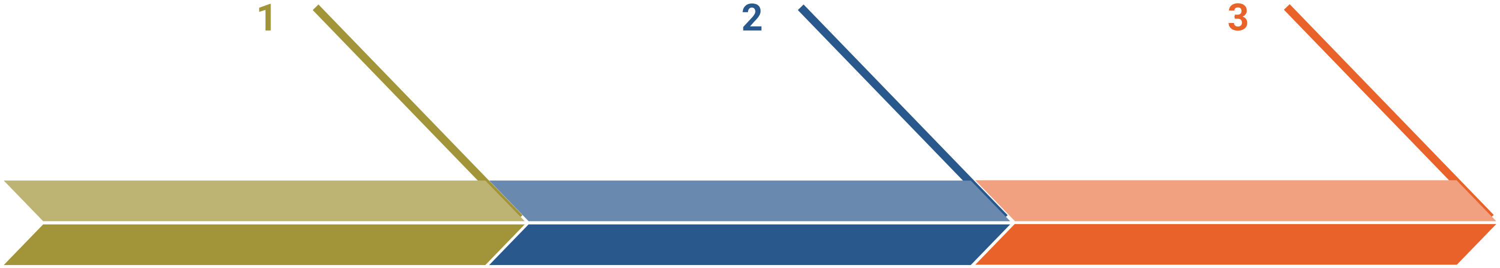
Carnival Corporation and subsidiaries receives a $5 million fine

Timeline of Events

October 2022

EyeMed Vision Settlement

EyeMed Vision Care Timeline



June 2020

Data Breach

January 2022

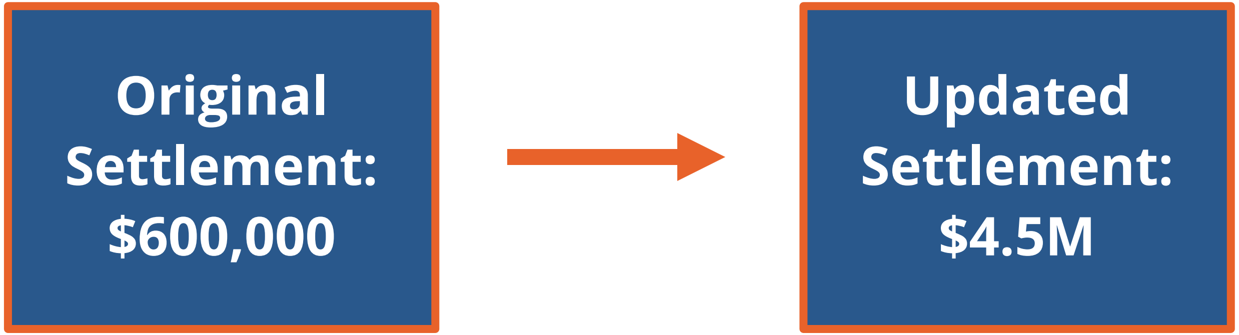
Original Settlement

October 2022

Updated Settlement

EyeMed Vision Care Summary

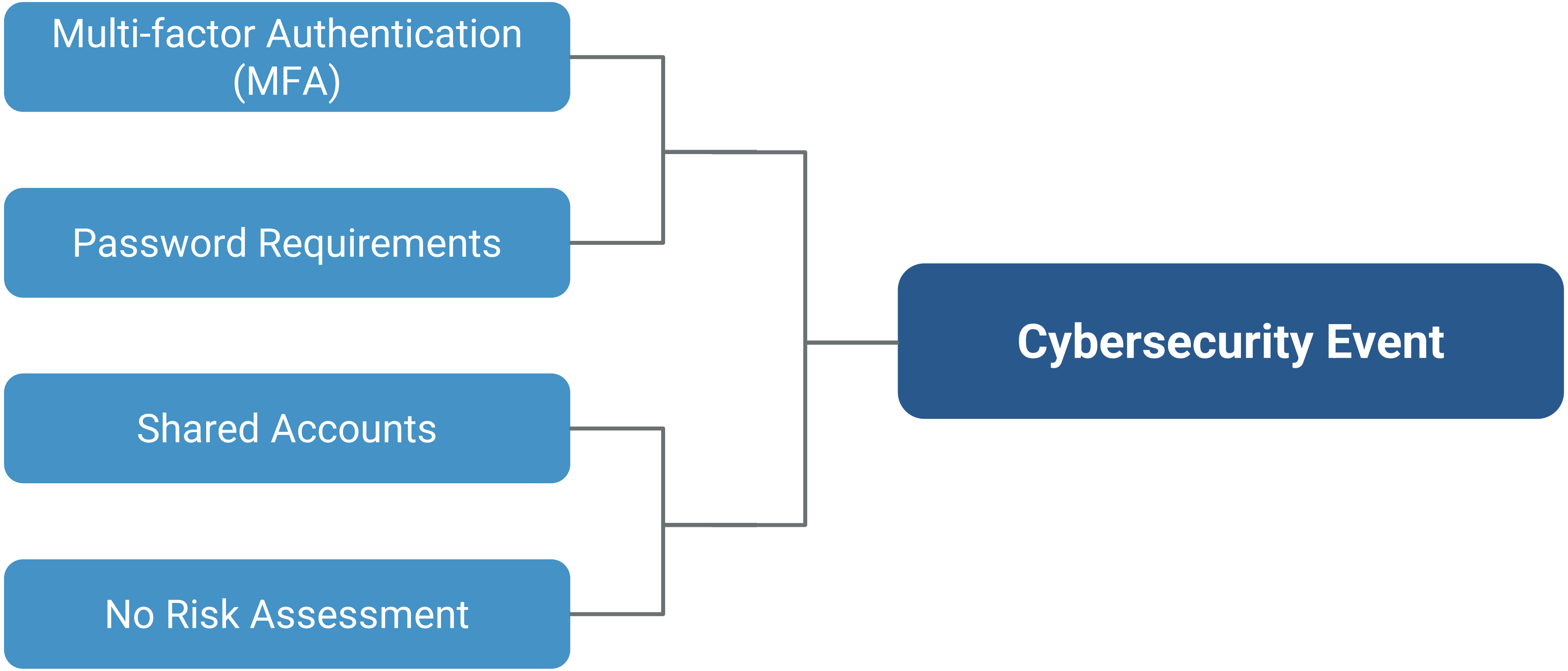
- Six years’ worth of consumer data
- Impacted 2.1 million individuals



Original Settlement: $600,000

Updated Settlement: $4.5M

EyeMed Vision Care Root Causes



Multi-factor Authentication (MFA)

Password Requirements

Shared Accounts

No Risk Assessment

Cybersecurity Event

Summary of Updates

JohnsonLambert
cpas + consultants

23 NYCRR 500

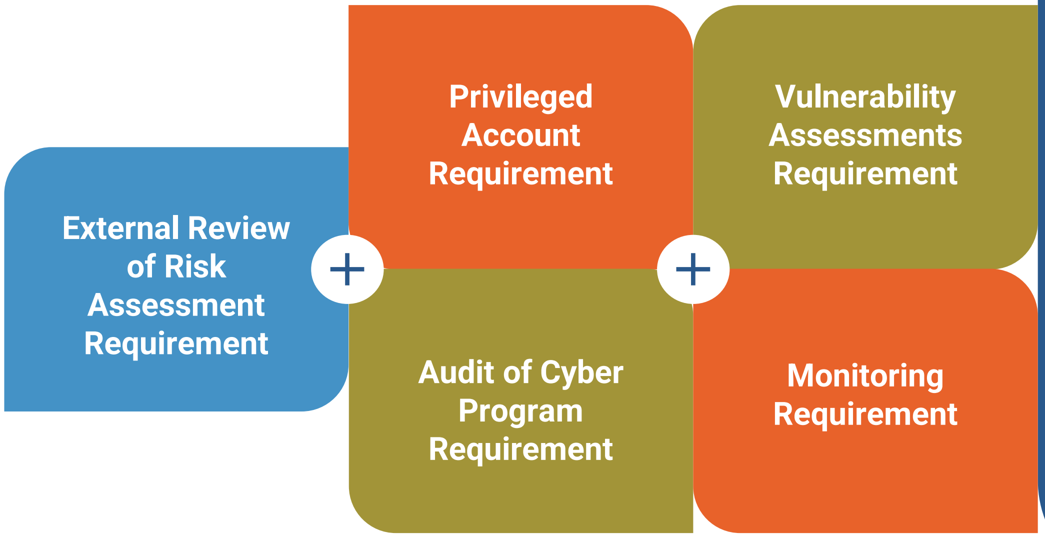
500.02	Cybersecurity Program
500.03	Cybersecurity Policy
500.04 a-b	Chief Information Security Officer (CISO)
500.05	Penetration Testing and Vulnerability Assessments
500.06	Audit Trail
500.07	Access Privileges
500.08	Application Security
500.09	Risk Assessment
500.10	Cybersecurity Personnel and Intelligence
500.11	Third Party Service Provider Security Policy
500.12	Multi-Factor Authentication
500.13	Limitations on Data Retention
500.14 a-b	Training and Monitoring
500.15	Encryption of Nonpublic Information
500.16	Incident Response Plan
500.17 a-b	Notices to Superintendent

23 NYCRR 500 Draft Amendment Updates

500.02	Cybersecurity Program
500.03	Cybersecurity Policy
500.04 a	~~Chief information security officer~~ Cybersecurity Governance
500.04 b	Chief Information Security Officer (CISO)
500.05	Penetration Testing and Vulnerability Assessments
500.06	Audit Trail
500.07	Access Privileges
500.08	Application Security
500.09	Risk Assessment
500.10	Cybersecurity Personnel and Intelligence
500.11	Third Party Service Provider Security Policy
500.12	Multi-Factor Authentication
500.13	~~Limitations on~~ Asset and Data Retention Management
500.14	~~Training and monitoring~~ Monitoring and Training
500.15	~~Encryption~~ Protection of Nonpublic Information
500.16 a-b	~~Incident Response Plan~~ Operational Resilience
500.17 a-b	Notices to Superintendent

New Type of Entity:
Class A

Class A (500.01) Definition + Obligations



External Review of Risk Assessment Requirement

+

Privileged Account Requirement

Audit of Cyber Program Requirement

+

Vulnerability Assessments Requirement

Monitoring Requirement

Class A companies mean those covered entities with:

1. Over 2,000 employees, including those of both the covered entity and all of its affiliates no matter where located; or
2. Over $1,000,000,000 in gross annual revenue averaged over the last three fiscal years from all business operations of the covered entity and all of its affiliates.

Governance

Policies (500.03)

That cybersecurity policy must be based on a risk assessment and address the following areas where applicable:

- (a) information security;
- (b) data governance and classification;
- (c) asset inventory, device management, and end of life management;
- (d) access controls, including remote access, 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;
- (n) incident response; and
- (o) vulnerability and patch management

Additional Policies (500.03)

- Updates to 500.03
  - End of life management
  - Remote access
  - Vulnerability and patch management
  - Annual policy review by senior governing body
- Inferred
  - Asset inventory (500.13)
  - Encryption (500.15)
  - Secure development standards (500.08)

Oversight + Independence (500.04 a-b)

- CISO independence
- Additional board reporting
  - Remediation plans
  - Cyber issues
  - Material gaps found in penetration tests and vulnerability scans (500.05)
- Board expertise
- CEO certification (500.17 b)

Class A: Audit of Cyber Program

Cyber program must have an independent audit conducted annually.

Technology

Assets (500.07) + Access (500.13)

- Asset inventory
  - Key tracking information
  - All types of assets
- Strengthen access controls
  - Privileged account definition
    - Limited to job function
    - Remote access
  - Periodic review
  - Passwords
  - MFA (500.12)

Class A: Privileged Accounts

- Monitor privileged access activity
- Password vaulting solution
- Automated method of blocking commonly used passwords

Operational Resilience (500.16 a-b)

- Business Continuity/Disaster Recovery (BCDR) Plan Requirements
  - Essential data and personnel
  - Communication plans
  - Back-up procedures
  - Identifying required third parties
- Tabletop exercises and IRPs
  - Test IR and BCDR plans with critical staff (including senior officers)
  - Restoring systems from backups
  - IRP must address ransomware and include recovery from backups
- Air gapped backup

Monitoring + Notification

Assessments (500.09)

- Risk Assessments
  - Tailored to company
  - Annual
- Impact Assessment
  - Requirement to conduct a impact assessment for all material changes

Class A: Risk Assessment

Risk assessment must be reviewed by an external party every 3 years.

Monitoring + Training (500.14)
Testing (500.05)

- Monitor and filter emails
- Cyber training expanded
  - Phishing
  - Exercises/ simulations
- Annual penetration testing
- Regular vulnerability testing
  - Material gaps found must be documented/ reported to the board and senior management

Class A: Monitoring

- Endpoint detection must be implemented to monitor network
- Solution must include centralized logging and security event alerting

Class A: Vulnerability Assessments

- Weekly scans or reviews of information systems

Notification (500.17 a-b)

72 hours of any unauthorized access to privileged accounts or deployment of ransomware within a financially significant system

24-hour notification obligation for any extortion payment connected to a cybersecurity event

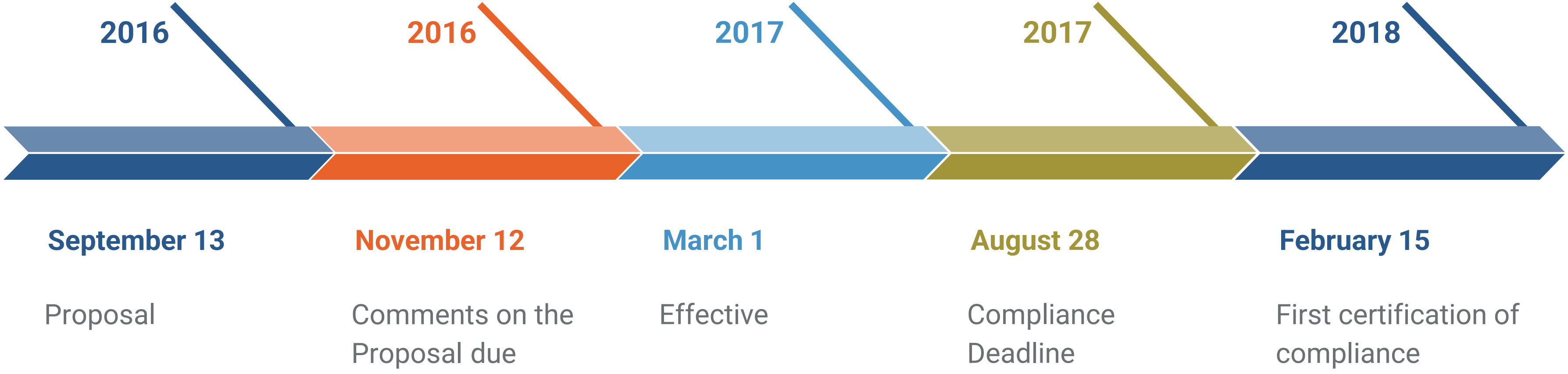
30-day reporting requirement explaining why payment was necessary, alternatives that were considered, and sanctions diligence that was conducted

April 15th: Annual submission to superintendent

Adoption Timeline

JohnsonLambert
cpas + consultants

First Amendment



2016

September 13

Proposal

2016

November 12

Comments on the Proposal due

2017

March 1

Effective

2017

August 28

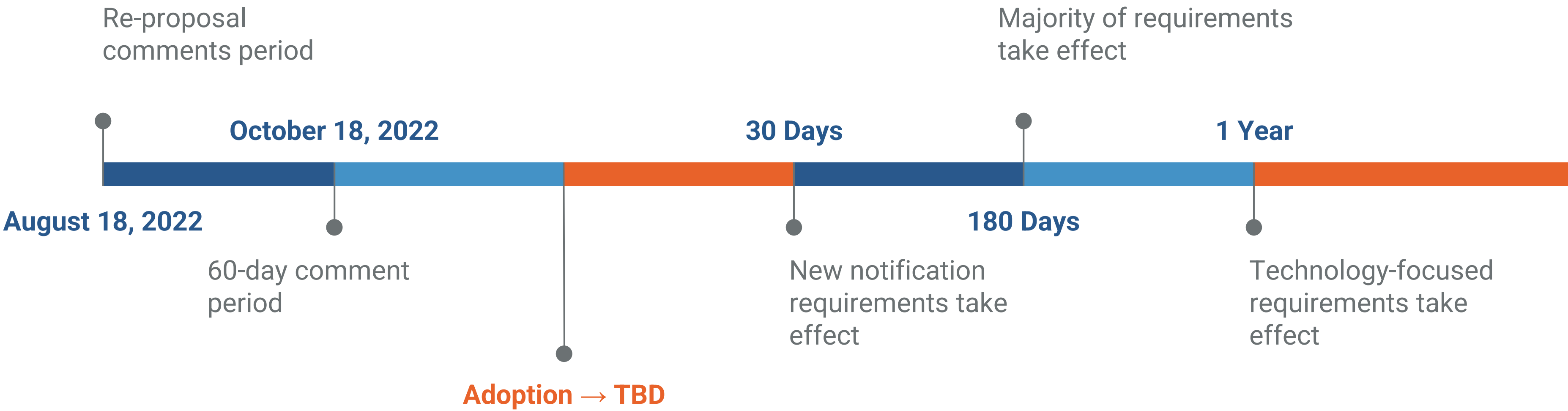
Compliance Deadline

2018

February 15

First certification of compliance

Draft Amendment



Re-proposal comments period

August 18, 2022

October 18, 2022

60-day comment period

Adoption → TBD

30 Days

New notification requirements take effect

Majority of requirements take effect

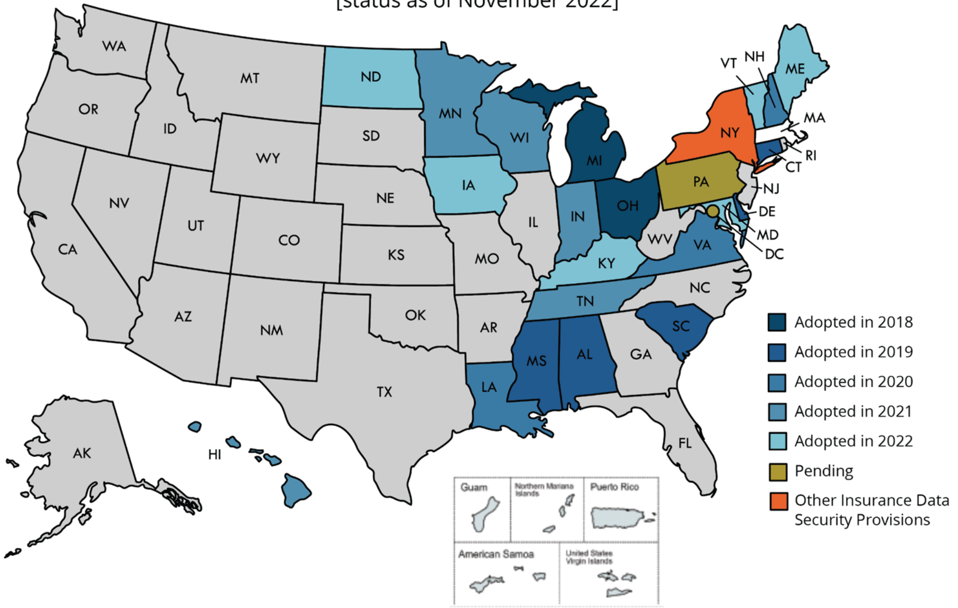
180 Days

1 Year

Technology-focused requirements take effect

NAIC Data Security Model Law: Adoption Status

Implementation of Model Act #668
Insurance Data Security Model Law
[status as of November 2022]



This map represents state action or pending state action addressing the topic of the model. This map does not reflect a determination as to whether the pending or enacted legislation contains all elements of the model or whether a state meets any applicable accreditation standards.

Adopted Model Law:

- Alabama
- Connecticut
- Delaware
- Hawaii
- Indiana
- Iowa
- Kentucky
- Louisiana
- Maine
- Maryland
- Michigan
- Minnesota
- Mississippi
- New Hampshire
- North Dakota
- Ohio
- South Carolina
- Tennessee
- Vermont
- Virginia
- Wisconsin

Pending Adoption:

- Pennsylvania
- DC

NYDFS Cybersecurity Regulation:

- New York

FAQ + Takeaways

JohnsonLambert
cpas + consultants

FAQ

1. When will the draft amendment take effect?
2. Since this is currently in draft -- will the final amendment be very different?
3. How long do companies have to become compliant with the new requirements?
4. Are there any exceptions?
5. Cyber insurance? Link to whitepaper

Takeaways

- Perform Gap Analysis
- Determine Road Map
- Consider a Cyber Pre-Assessment

Questions

JohnsonLambert
cpas + consultants