Cybersecurity Regulations: New York and Beyond

Cailie A. Currin, President

Currin Compliance Services, Inc.

AFA Spring Symposium: Compliance
May 24, 2017

Life • Health • Annuity

Compliance you can trust. Service you can rely on.

www.currincompliance.com (518) 692-2494

The Regulation

- Official reference: 23 NYCRR 500
  - Note this is Financial Services Regulation not Insurance

518-692-2494
CurrinCompliance.com

What are we talking about?

- Cyber Security Program
  - Designed to protect the confidentiality, integrity and availability of information systems.
- "Cybersecurity Event"
  - "any act or attempt, successful *or unsuccessful*" (emphasis added)
- Strict 72-hour notification standard
  - Reporting is required cybersecurity events, including unauthorized attempts to access your systems even if unsuccessful.

518-692-2494
CurrinCompliance.com

Regulatory Philosophy

New York is a “global financial powerhouse for the entire planet and it has a responsibility to take the lead in setting an example.”

Antony Haynes, Associate Dean and head of cybersecurity and data privacy programs at Albany Law School. *Financial Advisor*, March 30, 2017.

Regulatory Philosophy (cont.)

"New York is creating a standard that will probably be a catalyst for a national change."

John Cunningham, chief information security officer at Docupace Technologies.
Investment News, January 17, 2017

518-692-2494
CurrinCompliance.com

Does the regulation apply to you?

- Are you licensed in NY?
  - Yes
- No office in NY, but transact business in state?
  - Yes
- Do you have fewer than 10 employees?
  - Tentative no… includes independent contractors
- Do you have less than $5 million in gross revenue in each of the last three years from NY?
  - Tentative no, and…
- Do you have less than $10 million in total assets?
  - No

518-692-2494
CurrinCompliance.com

Core Requirements

- Enterprise-wise cybersecurity program and policy
- Designate a CISO (qualified chief information security officer)
- Maintain a cybersecurity program to protect the confidentiality, integrity and availability of information system, including nonpublic information
- Respond to identified or detected cybersecurity events to mitigate any negative effects

518-692-2494
CurrinCompliance.com

Core Requirements (cont.)

- Demonstrate an ability to recover from cybersecurity events and restore normal operations

- Fulfill regulatory reporting obligations

518-692-2494
CurrinCompliance.com

Important Dates: Licensed in NY

- February 16, 2017: DFS finalized release
- March 1, 2017: Effective date
- August 28, 2017: Written cybersecurity policy
- February 15, 2018: First annual certification of compliance must be submitted
- March 1, 2018:
  - CISO reporting requirement
  - Penetration testing and vulnerability assessment
  - Regular risk assessment
  - Multi-factor authentication
  - Cybersecurity awareness training
- September 1, 2018
  - Audit trail in place
  - Application security
  - Limitations on data retention
  - Monitoring procedures
  - Encryption of nonpublic information
- March 1, 2019
  - Third Party service provider security policy.

518-692-2494
CurrinCompliance.com

Compliance Philosophy

"The cost of a data breach, the fines associated with non-compliance and having premiums increase within our insurance portfolio is much higher than the upfront investment in time and energy required to be compliant."

David Derigiotis, director of professional liability and corporate vice president at Burns & Wilcox, insurance broker and underwriting manager.

518-692-2494
CurrinCompliance.com

What should we do first?

- Designate a Chief Information Security Officer
  - Can be employed by an affiliate
  - Title is not the mandate – functional responsibilities are

518-692-2494
CurrinCompliance.com

What other resources are required?

- Right people, resources and training
- Qualified cybersecurity personnel or third-party providers
- Oversight of cybersecurity functions
- Access, secure and encrypt NPI
- Broad audit trail of activities involving NPI
- Implement rigorous third-party cyber risk management policies and procedures
- Effective incident response program including notification to DFS of material cyber events

518-692-2494
CurrinCompliance.com

Risk Assessments

- Purpose: to design a program particular to your organization
- Realistic assessment of cyber risk and NPI storage, systems and utilization
- Controls can be revised and developed as business or technology evolves

518-692-2494
CurrinCompliance.com

Notification to Superintendent

- As soon as possible, no later than 72 hours from a determination that a cybersecurity event has occurred, if
  - Notice is required to another governmental body, self-regulatory agency or any other supervisory body, or
  - There is a reasonable likelihood of material harm to a material part of normal operations
- Annually by February 15 Compliance Certification

518-692-2494
CurrinCompliance.com

Annual Certification of Compliance

- Chair of the Board of Directors or Senior Officer(s) certifies:
  - Review of documents, reports, certifications and opinions
  - To the best of the Board/Senior Officer(s) knowledge, the cybersecurity program is in compliance
  - Must be a Board Resolution or a Compliance Finding that is the foundation for the signature.

518-692-2494
CurrinCompliance.com

Questions?

518-692-2494
CurrinCompliance.com

Thank you!