capitalcompliance EXPERTS

CYBERSECURITY 101

NEW YORK STATE DEPT OF FINANCIAL SERVICES REQUIREMENTS FOR FINANCIAL SERVICES COMPANIES

The New York State Department of Financial Services' new Cybersecurity Requirements for Financial Services Companies came into effect on March 1, 2017, with many transition dates for different requirements. By February 15, 2018, all covered entities must certify that they comply with the law. There is no time to waste.

Covered Entities include any business that requires authorization under New York State's Banking Law, Financial Services Law, or Insurance Law.

To comply with the law a Covered Entity is required to have a Cybersecurity Program to protect the Confidentiality, Integrity, and Availability (CIA) of customer data or NonPublic Information as the law calls it.

DEADLINE:
1st certification

MSBs need to assess their structures and operations and determine what policies, procedures and controls they need to meet these new requirements.


capitalcompliance EXPERTS

CERTIFICATE OF COMPLETION

John Smith

on this date

05/16/17

has successfully completed the following:

Financial Services Cybersecurity Principles

CAMS Certified Anti-Money Laundering Specialist

Debbie L. Owens, CAMS
Director of Compliance

THE LAW REQUIRES A COVERED ENTITY TO:

- Conduct a Risk Assessment upon which program is based. Periodic risk assessments are required.
- Appoint a Chief Information Security Officer (CISO) or Responsible Individual by August 2017 to oversee, implement and enforce the program. Employees that have roles under the program must be qualified for the assignments.
- Implement written cybersecurity policies approved by Board or Senior Official.
- Dispose of customer data periodically in secure manner.
- Develop an Incident Response Plan.
- Report cyberattacks to Department of Financial Services within 72 hours of discovery of attack. The attack need not be successful.
- Have standards and procedures for internally generated applications.
- Have guidelines to evaluate, assess and test security of 3rd party applications.
- Monitor and conduct regular penetration testing to assess effectiveness of program.
- Implement a policy to Monitor and Limit User Activity and Detect Unauthorized Access.
- Provide regular training so staff can identify, prevent, respond to and recover from cybersecurity threats. The CISO must also take steps to maintain current knowledge and be abreast industry developments.
- Implement encryption and authentication policy.

A Covered Entity is required to provide an Annual report to its Board or governing body on the program and any material cybersecurity risks.

By February 15, 2018, a covered entity must certify to the Department of Financial Services that it complies with the law. All records that support the certification must be maintained for five years.

REPORT CYBER RISKS

The law has many specific requirements that must be met and MSBs that wait until the last minute to develop their Cybersecurity Program will could be facing penalties. Exemptions provided are limited to specific

provisions and all covered entities now must watch the clock.

If you would like help with developing your Cybersecurity Program, contact us. We are CAMS certified and would love to help.

CONTACT US

(855) 922-4325
CapitalComplianceExperts.com