New York Cybersecurity Regulation for Financial Institutions Goes Into Effect

By: Jordan Meddy

GSB Contact:

Sy H. Bucholz
Washington, D.C.
sbucholz@gsblaw.com
212.965.4531

BEIJING

NEW YORK

PORTLAND

SEATTLE

WASHINGTON, D.C.

- "First-in-the-Nation" Rule promulgated by the New York State Department of Financial Services (DFS) aims to protect consumer data and ensure the safety and soundness of the State's financial services industry.

- Regulation became effective March 1, 2017.

- Affected parties have anywhere from 180 days to two years to comply with the various requirements.

Who is covered by the Regulation?

Any entity operating under or required to operate under a license, permit, or similar authorization under the New York State Banking Law, Insurance Law, or Financial Services Law (Covered Entities).

- Covered Entities include banks, trusts, budget planners, check cashers, credit unions, money transmitters, licensed lenders, and mortgage brokers.

- Covered Entities DO NOT include broker-dealers or registered investment advisors.

- Exemptions to certain requirements apply to Covered Entities with:

    - Fewer than 10 employees including any independent contractors, or
    - Less than $5,000,000 in gross annual revenue in each of the last three fiscal years, or
    - Less than $10,000,000 in year-end total assets

What is required?

- Each Covered Entity must implement and maintain a Cybersecurity Program designed to protect the confidentiality, integrity, and availability of its information systems. This Program should be based on a periodic

Risk Assessment performed by each Covered Entity, designed to identify and assess internal and external cybersecurity risks, and should include monitoring and testing at least periodically.

- Each Covered Entity must implement and maintain a written Cybersecurity Policy or Policies, setting forth the policies and procedures for the protection of its information systems and the information stored on those systems. The Cybersecurity Policy or Policies should address to the extent applicable to a Covered Entity's operations:
    - Information Security
    - Data Governance and Classification
    - Asset Inventory and Device Management
    - Access Controls and Identity Management
    - Business Continuity and Disaster Recovery Planning
    - Systems and Network Security/Monitoring
    - Customer Data Privacy
    - Vendor and Third Party Service Provider Management
    - Risk Assessment
    - Incident Response

- Each Covered Entity must designate a Chief Information Security Officer (CISO), responsible for overseeing and implementing the Cybersecurity Program and enforcing its Cybersecurity Policy. The CISO is responsible for reporting in writing at least annually to the Covered Entity's board of directors or equivalent governing body on the Cybersecurity Program and material risks.

- Each Covered Entity must report the occurrence of any material cybersecurity attack to the DFS Superintendent.

Please contact us for more information on the applicability and requirements of this new DFS regulation.