



# New Cybersecurity Regulation Financial Services Companies

Because cyber hacking constitutes a major threat to United States financial markets, the New York State Department of Financial Services (DFS) has issued new regulation requiring more than 3,000 banks, insurance companies and other financial services organizations to comply with new cyber security rules. The DFS plans were formally announced by Gov. Andrew Cuomo on February 16, 2017; the final version of the new Regulation 23 NYCRR 500 can be found at <http://www.dfs.ny.gov/legal/regulations/proposed/rp500t.pdf>. The effective date for the requirements is March 1, 2017 and financial services companies are required to be compliant within 180 days. Boards or Senior Management will be required to sign and submit an annual Certification of Compliance with the Cybersecurity regulation by February 18, 2018.

## Some of the key requirements of the regulation are:

- Having a formal Cybersecurity Program based on the covered entity's risk assessment and a written Cybersecurity Policy
- Designating a Chief Information Security Officer (CISO)
- The CISO must report in writing at least annually to the board of directors or equivalent governing body
- Conducting routine periodic Penetration Testing and Vulnerability Assessments
- Maintain audit trails designed to detect and respond to Cybersecurity events
- Completing a Cybersecurity Risk Assessment
- Having a Third Party Service Provider Security Policy and effective controls
- Use of Multi-Factor Authentication
- Encryption of Non-Public Information
- Limitation on Data Retention
- Effective Training and Monitoring of Cybersecurity
- Effective controls for Application Security and Access Privileges
- Incident Response Plan and Notification of Incidents

## Freed Maxick can help your financial institution assure compliance with the new DFS Cybersecurity regulation. Freed Maxick provides a full portfolio of Cybersecurity Services including:

- DFS Cybersecurity Compliance Gap Assessment
- Cybersecurity Program Implementation Services including:
  - Program design and implementation consulting and project management
  - Policy, Procedure and Controls documentation consulting
  - Third Party Service Provider Risk Management consulting
  - Incident Response Plan consulting
- Cyber Vulnerability Assessments and Penetration Testing
- Cybersecurity Awareness Training
- Cybersecurity and IT Risk Assessments
- Cybersecurity Program Compliance Audits including:
  - Attestations on Compliance
  - Service Organization Control 1, 2 and 3 Audit Reports

Trust earned.



FREEDMAXICK.COM | Buffalo Batavia Rochester Syracuse | 800.777.4885



Freed Maxick is the brand under which Freed Maxick CPAs, PC, provides services to its clients. Square logo, FreedMaxick, and "Trust Earned." are registered trademarks of Freed Maxick CPAs, PC.