DFS: Who we Regulate

Through chartering, licensing, examination, regulation and enforcement, DFS supervises financial services companies in the State of New York, including:

1,500 banking and other financial institutions with assets of more than $2.6 trillion

1,400 insurance companies and 300,000 individual insurance licensees with assets of more than $4.3 trillion

New York oversees more domestic insurers than any other state

Cybersecurity Division

In 2019, DFS announced the first-in-the-nation Cybersecurity Division to be established at a banking or insurance regulator.

- To protect consumers and industry by improving cybersecurity across the financial services industry.
- Oversees examinations and enforcement related to DFS's cybersecurity regulation.
- Issue guidance to industry and consumers on DFS's cybersecurity regulation, and cybersecurity risks and best practices.

The Part 500 Cyber Reg

- 23 NYCRR 500: First-in-then-nation financial services cybersecurity regulation
- First proposed: September 2016
- Two rounds of notice and comment
- Effective March 1, 2017*
- Basis for NAIC & CSBS model cybersecurity laws and FTC Safeguard regulation

*The provisions of the NYDFS Cyber Reg become effective over a two-year transition period.

Who is required to comply

Who ***is***?

- Broad coverage; Any entity that is chartered, licensed, or approved to operate in NYS by DFS
- Including:
- Banks
- Check cashers
- Insurance companies
- Insurance producers
- Money transmitters
- Trust companies
- Virtual currency companies

- Who ***is not***?
  - Third Party Service Providers are not directly regulated by NYSDFS
  - Examples include:
    - Amazon Web Services/Google/Microsoft
    - Dell
    - FiServ
    - Jack Henry
- Using a third party does not exempt an entity from the requirements of this regulation

What is being protected? Nonpublic Information (500.01)

All electronic information that is not Publicly Available Information and is:	
Business Related Information	Tampering with which, or unauthorized disclosure, access or use of which, would cause a **material adverse impact** to the business, operations or security of the Covered Entity
Personal Identifiable Information or **(PII)**	Specifically defined but including: i. social security number ii. drivers' license number iii. account number, credit or debit card number iv. any security code, access code or password that would permit access to an individual's financial account v. biometric records
Healthcare Information or **(PHI)**	Specifically defined but Including created by or derived from a health care provider that relates to: i. the past, present or future physical, mental or behavioral health or condition of any individual or a member of the individual's family ii. the provision of health care to any individual, or iii. payment for the provision of health care to any individual.

Cybersecurity Governance

- Creates a governance structure where cybersecurity is a focus throughout the organization.
- Examples include
  - Certification of Compliance
  - Board approval of policies and procedures
  - A CISO that reports directly to the board
  - Training for all employees on cybersecurity awareness

Cybersecurity Program

- Cybersecurity program is key for effective security management practices and controls
- People, Processes, Technology
- Risk assessment is the cornerstone to cybersecurity
- Policy & procedure creates the governance structure to define the control environment.
- Financial Services Toolkit: https://www.dfs.ny.gov/consumers/small_businesses/cybersecurity

Noteworthy Cyber Requirements

- Data Governance/Classification Policy (500.03(b)),
- Customer data privacy policy (500.03(k))
- Penetration Testing and Vulnerability Assessment (500.05)
- Audit Trail (500.06)
- Limitations on Data Retention (500.13)
- Incident Response (500.16)

Cyber Reg Exemptions 500.19

- Small Business Exemption - 500.19(a)
  - <10 Employees
  - <$5M gross annual revenue in each of the last 3 years
  - <$10M in year-end total assets
- No systems or non-public information - 500.19(c)

- These are partial exemptions
- To file an exemption, go to https://myportal.dfs.ny.gov/web/cybersecurity/

Cyber Reg Exemptions 500.19

23 NYCRR 500

500.02- Cybersecurity Program**
500.03- Cybersecurity Policy**
500.04- Chief Information Security Officer*
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
500.12- Multi-Factor Authentication*

500.13- Limitations on Data Retention
500.14- Training and Monitoring*
500.15- Encryption of Nonpublic Information*
500.16- Incident Response Plan**
500.17- Notices to Superintendent
500.18- Confidentiality
500.19- Exemptions
500.20- Enforcement
500.21- Effective Date
500.22- Transitional Periods
500.23- Severability

Bold all entities are required.
* Exempt 500.19 (a),(c) ** Exempt 500.19 (c)

NEW YORK STATE OF OPPORTUNITY. Department of Financial Services

Notices to Superintendent 500.17

1. Annual Compliance Certification

- ✓ Attests to compliance for the prior calendar year, beginning in 2018
- ✓ Submitted annually by April 15
- ✓ Signed by the Chairman of the Board of Directors or a Senior Officer
- ✓ All records supporting a certificate of compliance must be maintained for a *minimum* of 5 years
- ✓ See Appendix A for Form Letter

2. Cybersecurity Events
   1) Reported to other agency/body
   2) Material harm to business operations

- ✓ Must be reported within 72 hours of determining an event is has occurred:
  - □ Reported to gov't body, regulatory agency or supervisory body
  - □ Has a reasonable likelihood of materially harming any material part of the normal operation(s) of the covered entity

3. Notice of Exemption

- ✓ See Appendix A for Form Letter