CCLS CORE COMPLIANCE & LEGAL SERVICES, INC.

Risk Management Update
October 2017

New York's Cybersecurity Requirements for Financial Services Companies

In 2017, the State of New York's Department of Financial Services ("DFS") adopted new requirements for financial services companies ("Covered Entities")[1] to create and maintain robust cybersecurity policies and programs in a continuing effort to thwart cybercrimes and large scale cyber-attacks, address system vulnerabilities, and mitigate the effects of events that could compromise the security of personally identifiable information of clients.[2]

While the requirements under this regulation are not applicable to registered investment advisers ("RIAs"), it may impact those RIAs and/or investment adviser representatives ("IARs") who provide additional services, such as insurance services, which fall under the purview of DFS. In addition, RIAs may benefit from reviewing the rule for additional guidance to shore up their own cybersecurity program.

In this month's Risk Management Update we cover the main requirements of this DFS regulation, exemptions that may be available for Covered entities and agents, key dates that need to be monitored, and provide steps for Covered Entities to consider that will assist with ensuring compliance with the rule.

New York DFS Cybersecurity Requirements for Financial Services Companies

DFS is responsible for supervising a large swath of Covered Entities operating in the state of New York, including, but not limited to:

- Banks & Trust Companies
- Budget Planners
- Charitable Foundations
- Check Cashers
- Credit Unions
- Domestic Representative Offices
- Foreign Agencies
- Foreign Bank Branches
- Foreign Representative Offices
- Health Insurers, Accident and Related Entities
- Licensed Lenders
- Life Insurance Companies
- Money Transmitters
- Mortgage Bankers and Brokers
- Mortgage Loan Originators and Servicers
- New York State Regulated Corporations
- Premium Finance Agencies
- Private Bankers
- Property and Casualty Insurance Companies
- Safe Deposit Companies
- Sales Finance Companies
- Savings Banks
- Savings and Loan Associations
- Service Contract Providers

---

[1] The DFS defines a "*Covered Entity"* to mean: "any Person operating under or required to operate under a license, registration, charter, certificate, permit, accreditation or similar authorization under the Banking Law, the Insurance Law or the Financial Services Law."

[2] 23 NYCRR Part 500. *See* http://www.dfs.ny.gov/legal/regulations/adoptions/dfsrf500txt.pdf

Some of the main components of the DFS' required cybersecurity program include:

- Performing periodic risk assessments to identify and assess risks applicable to the safeguarding of non-public information stored in the firm's electronic network and storage systems;
- Creating and maintaining cybersecurity policies and procedures designed to protect such non-public information, detect cybercrimes, and promptly respond to and mitigate damage from, a cyber-attack;
- Appointing a Chief Information Security Officer ("CISO") to oversee the maintenance of the covered entity's cybersecurity program;
- Documenting and maintaining access privileges and application security;
- Conducting periodic penetration testing, vulnerability assessments and annual testing;
- Maintaining an audit trail (as outlined in 23 NYCRR Section 500.06); and
- Timely filing of all required reporting.

Possible Exemptions

Covered Entities may qualify for an exemption for part of the rule requirements if they meet the criteria outlined under 23 NYCRR Section 500.19(a)-(d),[3] as applicable. For example, below is list of the criteria that Covered Entities would need to meet in order to claim an exemption from most of the requirements ("limited exemption")[4]:

- Having fewer than 10 employees, including any independent contractors, of the Covered Entity or its affiliates (as such term is defined in the rule) located in New York or responsible for business of the Covered Entity;
- Receiving less than $5,000,000 in gross annual revenue in each of the last three fiscal years from New York business operations of the Covered Entity and its affiliates; or
- Having less than $10,000,000 in year-end total assets, calculated in accordance with generally accepted accounting principles, including assets of all affiliates.

If a covered entity verifies that it qualifies for a limited exemption under 23 NYCRR 500.19(e) it will need to file a Notice of Exemption with DFS on the DFS Web Portal.[5]

Upcoming Compliance Dates

Below is a list of important upcoming compliance dates applicable to the rule:

- **October 30, 2017 –** deadline for filing a Notice of Exemption required by 23 NYCRR 500.19(e), if applicable;

---

[3] *See* http://www.dfs.ny.gov/legal/regulations/adoptions/dfsrf500txt.pdf, page 11.
[4] Please note this only reflects one of the exemptions outlined in Section 500.19, others may apply.
[5] *See* http://www.dfs.ny.gov/about/cybersecurity.htm.

- **February 15, 2018** - Covered Entities are required to submit the first certification under 23 NYCRR 500.17(b) on or prior to this date;
- **March 1, 2018** - Covered Entities are required to be in compliance with the requirements of sections 500.04(b), 500.05, 500.09, 500.12 and 500.14(b) of 23 NYCRR Part 500;
- **September 3, 2018** - Covered Entities are required to be in compliance with the requirements of sections 500.06, 500.08, 500.13, 500.14(a) and 500.15 of 23 NYCRR Part 500; and
- **March 1, 2019** - Covered Entities are required to be in compliance with the requirements of 23 NYCRR 500.11.

Compliance Steps

Senior management of Covered Entities should consider taking the following steps:

1. Review the requirements and exemptions to determine applicability.
2. Work with operations and IT personnel to assess the cybersecurity risks of the firm.
3. Determine appropriate person to be the CISO.
4. Implement or enhance, as applicable, the firm's cybersecurity policies, procedures, and internal controls to meet the requirements of the DFS rule.
5. Adopt testing protocols to ensure ongoing compliance.
6. Maintain calendar to monitor and ensure timeliness of all required filings.

Conclusion

Cybersecurity continues to be a vital component of the protection of both firm and clients' non-public information. It is imperative that RIAs and other financial industry firms remain aware of, and maintain compliance with applicable rules and regulations to protect the integrity and security of such data.

For more information or for assistance with the review of the NY DFS rules, implementing cybersecurity policies and programs, and/or performing risk assessments and reviews, please contact us at info@corecls.com, at (619) 278- 0020 and visit us at www.corecls.com for additional information.

Author: Adam Stutz, Compliance Consultant; Editor: Tina Mitchell, Lead Sr. Compliance Consultant Core Compliance & Legal Services ("CCLS"). CCLS works extensively with investment advisers, broker-dealers, investment companies, hedge funds, private equity firms and banks on regulatory compliance issues.