CADWALADER

Cadwalader, Wickersham & Taft LLP
www.cadwalader.com

# The Clock Is Ticking: Companies Need to Comply Now with New DFS Cybersecurity Rules in New York

Strict new cybersecurity rules – described by the New York Department of Financial Services (DFS) as "first-in-nation" in terms of their scope and requirements – became effective in New York on March 1, 2017. Entities covered by the new rules ("covered entities") now have just months to comply – or potentially face harsh penalties.

## What Entities are Covered by the New Rules?

With limited exceptions, the rules apply to businesses regulated by the DFS, which include a wide range of insurance, banking, and financial services companies. Third party service provides, while not expressly covered by the rules, will also be required to adopt robust cybersecurity risk management programs if they wish to continue to do business with covered entities.

- Financial Institutions
- Banks
- Insurance Compaines

## What Happens if Covered Entities Fail to Comply with the New Rules?

It remains to be seen how aggressively the DFS will pursue entities that fail to comply with the new rules. However, the DFS has imposed large fines on financial institutions in other areas, such as with anti-money laundering laws. Under the rules, DFS can demand that covered entities produce for inspection all documents and information relevant to a covered entity's cybersecurity program.

## Interested in learning more?

Cadwalader would be pleased to present a customized CLE program in your office or as a webinar.

**Jennifer Olson**

**+1 212 993 2990**

**jennifer.olson@cwt.com**

# DEADLINES

The rules will be phased in over a period of two years after their effective date (March 1, 2017), with the following important deadlines for covered entities:

**1st Deadline**

## August 28, 2017

- Adopt written cybersecurity policies and procedures, including an incident response plan.
- Designate a Chief Information Security Officer (CISO) and retain qualified cybersecurity personnel.
- Notify DFS within 72 hours of determining that a cybersecurity event has occurred.
- Ensure that only appropriate personnel may access confidential non public data.

**2nd Deadline**

## February 15, 2018

- Submit annual compliance certifications, signed by a senior officer, to DFS.

**3rd Deadline**

## March 1, 2018

- Implement multi-factor authentication.
- Conduct regular penetration testing and risk assessments.
- Implement cybersecurity awareness training.

**4th Deadline**

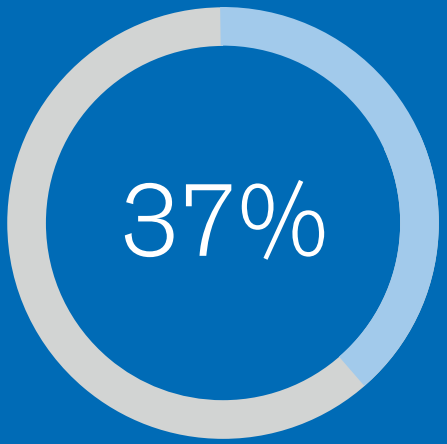
## September 1, 2018

- Encrypt confidential data
- Monitor user activity.
- Implement secure data disposal procedures.
- Maintain audit trails for network activity and significant transactions.

## Final Deadline

**March 1, 2019**

Adopt comprehensive cybersecurity risk management programs for third party service providers.




Only 37% of businesses report having a fully-operational incident response plan. (*Source: 2016 PwC survey of businesses*)

**Cadwalader's interdisciplinary cybersecurity team is led by:**


**John T. Moehringer**
*Partner – New York*
Intellectual Property
+1 212 504 6731
john.moehringer@cwt.com

**Joseph V. Moreno**
*Partner – Washington, DC*
White Collar Defense and Investigations
+1 202 862 2262
joseph.moreno@cwt.com

**Joseph Facciponti**
*Special Counsel – New York*
Corporate and Financial Services
Litigation and Regulation
+1 212 504 6313
joseph.facciponti@cwt.com