New York Finalizes Cybersecurity Regulation

McGlinchey Consumer Financial Services Alert

February 21, 2017

By: Peter L. Cockrell

Download this alert as a PDF.

Related Professionals

Peter L. Cockrell

Related Services

Consumer Financial Services Compliance

Cybersecurity and Data Privacy

On February 16, 2017, the New York State Department of Financial Services (NYDFS) issued a final cybersecurity regulation (Final Regulation) that will require covered entities to maintain a robust cybersecurity program.

The NYDFS originally issued a proposed regulation on September 13, 2016 (see our prior client alert on the subject here). In response to strong industry concern regarding its burdensome requirements, the NYDFS issued a revised proposed regulation on December 28, 2016 (see our prior client alert on the subject here). The NYDFS made changes in the revised proposed regulation to respond to industry concerns, but the revised regulation still presented significant compliance challenges.

The Final Regulation has largely been adopted as proposed in the revised regulation, but the NYDFS did make a few revisions. Among others, the NYDFS revised the small entity exemption to provide that the gross annual revenue threshold is limited to revenue from New York business operations of the covered entity and its affiliates. The Final Regulation also includes exemptions for certain insurance companies. We have prepared a comparison of the Final Regulation against the revised proposed regulation to illustrate the differences.

Effective Date and Transitional Periods

The Final Regulation becomes effective March 1, 2017. Covered entities will generally have 180 days from the effective date to comply. However, the Final Regulation includes several transitional periods for several key provisions.

Covered entities will have **1 year** from the effective date to comply with the following:

1. First CISO report to the board of directors
2. Penetration testing and vulnerability assessments
3. Risk assessment
4. Multifactor authentication
5. Cybersecurity training for all personnel

Covered entities will have **18 months** from the effective date to comply with the following:

1. Audit trail
2. Application security
3. Limits on data retention
4. Policies and procedures and controls for monitoring activity of authorized users
5. Encryption

Finally, covered entities will have **2 years** from the effective date to comply with the third-party service provider security policy requirement.

For further information on this topic, please contact a member of the firm's Consumer Financial Services Group.