NEW NY CYBERSECURITY REGS WILL HAVE NATIONAL REACH

This article first appeared in Law360, March 22, 2017

Cybercrime and identity theft pose an ever-increasing threat to the consumers of financial products and services. Current federal law requires financial institutions to implement information security programs to protect financial consumers' personal information. These requirements have provided financial institutions a risk-based, flexible approach to implementing safeguards that are reasonable and appropriate to the size and complexity of the institution. In a break from this risk-based approach, and to confront the rising threats faced by today's financial sector, New York Gov. Andrew Cuomo recently announced a cybersecurity regulation for New York's financial services sector which took effect on March 1, 2017.[1] The regulation will require financial institutions to implement specific, enumerated safeguards to detect, thwart and report cyber incidents.[2]

Given the national reach of the New York Department of Financial Services[3] (NYDFS), the impact of the new regulation will be felt far beyond the state of New York and may drive similar changes to other state and federal information protection laws, becoming the baseline standard for the industry. Almost any entity that operates under a license, registration, charter, certificate, permit, accreditation or similar authorization under the banking, insurance and financial services laws of New York is covered by the regulation. There are few exemptions (see below). The new regulation's specific requirements will also impact the financial sector service provider community, including IT service providers, law and accounting firms, and a host of other vendors.

Generally speaking, the regulation requires banks, insurance companies and other financial services institutions regulated by the NYDFS to establish and maintain cybersecurity programs designed to protect consumers' private data and ensure industry safety. The regulation includes certain minimum standards and encourages firms to keep pace with technological advances. Such broad requirements are common features of cybersecurity regulations across different industries, including the Gramm-Leach-Bliley Act's[4] (GLBA) safeguards rule[5], which is the backbone of current federal cybersecurity regulation for the financial sector. However, the New York regulation raises the bar in several notable ways, many of which may portend the future of cybersecurity regulation in general.

Enacted in 1999, a prominent provision of GLBA led to the promulgation of the safeguards rule, which became effective in 2003. In a likely case of regulatory language-borrowing, the safeguards rule included elements familiar in 1996's Health Insurance Portability and Accountability Act's security rule[6], including requirements to conduct risk assessments, analyze anticipated threats to sensitive information, and implement comprehensive, written information security programs, and administrative, technical and physical safeguards. The safeguards rule also presciently required financial institutions to assess and manage third-party risk to customer data, a requirement that arguably has moved the information security dial across industries servicing the financial sector, including the legal industry.

For more information, please contact:

Romaine Marshall
801.799.5922
rcmarshall@hollandhart.com

Matt Sorensen
801.799.5957
cmsorensen@hollandhart.com

In the 15 years since the safeguards rule's adoption, numerous financial regulators have issued guidance to help the financial sector keep abreast with technological advances and the changing threat environment. Such guidance has dealt with multifactor authentication, identity theft, emerging threats to widespread technologies, and the retirement of popular operating systems. In what might be a further sign of GLBA's lagging pace, in August 2016 the Federal Trade Commission, which regulates entities not already assigned by GLBA to federal banking agencies or other regulators, requested public comment on the safeguards rule.[7] The public comment is focused on the safeguards rule's economic benefits and disadvantages and whether state or local laws conflict with the rule.

Proponents of GLBA's risk-based, flexible approach point out that the lack of specificity in the safeguards rule leaves financial institutions free to avoid one-size-fits-all approaches, allowing them to adopt information security programs that are reasonable and appropriate given the size and complexity of the institution. The approach taken by the NYDFS indicates that many specific information security practices and safeguards are so fundamental and necessary that they are no longer optional under a flexible standard.

To raise the bar the New York regulation requires covered entities to:

- Include data governance, data classification, asset and device inventory, business resiliency (business continuity and disaster recovery), and incident response in written information security policies
- Develop the equivalent of risk treatment plans as a result of the risk assessment
- Comply with governance and staffing requirements — including appointment of a chief information security officer or equivalent, by August 2017
- Implement continuous vulnerability monitoring, or at a minimum conduct annual penetration testing and biannual vulnerability assessments, presumably both internal and external vulnerability scans
- Maintain transaction and server logs that would detect and respond to cybersecurity events
- Maintain application security written procedures, guidelines and standards
- Use multifactor authentication or risk-based authentication
- Destroy nonpublic information periodically and securely
- Implement controls, including encryption or compensating controls
- Establish a written incident-response plan
- Provide cybersecurity personnel with specific training relevant to cybersecurity risks, and verify that cybersecurity employees maintain a knowledge of current threat environments and evolving safeguards and security tactics
- Notify NYDFS of any breaches within 72 hours.

Although the regulation took effect on March 1, 2017, it includes transition periods of between one and two years for most requirements. Even with the staggered compliance

dates, however, full compliance with these requirements will be challenging.

Some of the regulation's requirements still apply to entities that seek exemption. These requirements include conducting a risk assessment, implementing written policies and procedures to secure nonpublic information that is accessible to, or held by, third-party services providers; and establishing policies and procedures for the secure disposal of nonpublic information. Some persons or entities will be exempt from most of the regulation's requirements: small covered entities of "fewer than 10 employees" or "less than $5 million in revenue in each of the last three fiscal years," designees covered by another covered entity, entities that do not possess or handle nonpublic information, and captive banks or insurance companies that only handle the nonpublic information of the corporate parent company.[8] Exempted covered entities must still file a certificate of exemption with NYDFS within 30 days.

The impact of the regulation on financial companies in New York is clear. Less clear however, is the impact of the regulation on other regulated industries and other U.S. jurisdictions. The growth and popularity of data breach notification requirements in the U.S. may illustrate the regulation's future impact. In 2002 California enacted SB 1386[9], the nation's first state data breach notification law. Since then 46 other states, Washington, D.C., and three U.S. territories have enacted similar laws. Both HIPAA and GLBA have been influenced by the proliferation of data breach notification requirements. Several types of data protection laws that have grown popular across the U.S. originated in Massachusetts.

The requirements in the regulation are widely accepted as reasonable and prudent among information security professionals.[10] The requirements can easily be referenced to several popular control frameworks and standards, including ISO 27001[11], CIS Critical Controls[12] and NIST SP 800-54[13]. The regulation does not set forth new or original safeguards, rather it explicitly mandates many safeguards already well-known to information security community. It is in its specificity that the regulation stands unique among its peers, and it will likely pave the way for similar specificity in future regulation.

—By Romaine Marshall and Matt Sorensen, Holland & Hart LLP

Romaine Marshall is a partner and Matt Sorensen is an associate at Holland & Hart in Salt Lake City.

[1] http://www.dfs.ny.gov/about/press/pr1702161.htm

[2] 2017 NY REG TEXT 437094

[3] http://www.dfs.ny.gov/

[4] 15 USC 6801, et. sec.

[5] e.g. 12 CFR Pt. 30, App. A

[6] 45 CFR Pt. 160, 162, 164.

HOLLAND&HART LLP

[7] https://www.ftc.gov/news-events/press-releases/2016/08/ftc-seeks-comment-safeguards-rule

[8] Id., infra. fn. 2.

[9] Cal. Civ. Code 1798.29, et. seq.

[10] The ongoing debate within the information security community over the effectiveness, efficacy and viability or information security risk assessments notwithstanding.

[11] Available for purchase at http://webstore.ansi.org/

[12] https://www.cisecurity.org/critical-controls.cfm

[13] http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf