THOMSON REUTERS
Westlaw®

3 key areas where the NYDFS ups the ante on cybersecurity

By Elizabeth E. McGinn, Esq., and David Rivera, Esq., *Buckley LLP*, and James Shreve, Esq., *Thompson Coburn LLP*

JUNE 24, 2019

On March 1, the two-year transitional period under the New York State Department of Financial Services' "Cybersecurity Requirements for Financial Services Companies" regulation expired, making all requirements effective.

The cybersecurity regulation marks a shift in the governance of cybersecurity. Previously, governmental agencies largely scrutinized a cybersecurity program after a security incident occurred, and even then focused primarily on the company's notification to affected consumers whose personal information may have been compromised.

Now, New York requires businesses to certify annually that they have proactively built an appropriate security program and infrastructure with several concrete elements to protect sensitive information.

While financial institutions face parallel requirements under the federal Safeguards Rule[1] enacted under the Gramm-Leach-Bliley Act, the cybersecurity regulation differs in two ways. First, it is considerably more prescriptive than the existing federal requirements because it demands that businesses adopt specific cybersecurity controls. Second, the cybersecurity regulation seeks to protect a broader range of information than the Safeguards Rule, in line with how cybersecurity threats have evolved over the past 15 years.

Certain elements of the cybersecurity regulation are present in other regulations and guidance, such as the Federal Financial Institutions Examination Council's Information Technology Examination Handbook and Massachusetts' standards for the protection of its residents' personal information.

However, the cybersecurity regulation goes beyond previous issuances by requiring more specific security controls in a greater number of risk areas.

This commentary will first provide background on the legal and regulatory requirements that preceded the cybersecurity regulation and analyze, in turn, how the regulation differs from its formative predecessors in its approach to three key areas of cybersecurity compliance. It will also discuss how those differences are important for financial institutions doing business in New York and beyond.

BACKGROUND

The cybersecurity regulation imposes another regulatory layer over existing federal rules under which covered entities are regulated.

All financial institutions must comply with the Safeguard Rule, which:

- Requires the creation of a comprehensive information security program containing "administrative, technical, and physical safeguards" appropriate to the entity's risk profile and the sensitivity of any customer information it maintains.
- Affords broad discretion to the financial institution to design an effective security program.
- Requires that the security program address a few particular elements, but allows the institution to determine the appropriate controls.

Some have lauded this less prescriptive and risk-based approach. However, detractors argue that the Safeguards Rule's deferential approach, together with consent orders (entered in response to enforcement actions) that do not provide significant factual details about alleged violations of the rule, may not provide enough concrete guidance on regulators' expectations for a security program.

Previously, governmental agencies largely scrutinized a cybersecurity program after a security incident occurred, and even then focused primarily on the company's notification to affected consumers whose personal information may have been compromised.

For depository institutions, the FFIEC Handbook's information security booklet lists some of the regulatory expectations of the Safeguards Rule's cybersecurity requirements. The NYDFS cybersecurity regulation, meanwhile, differs from the federal

approach by listing specific regulatory expectations for security controls directly as a point of compliance, rather than presenting them as guidance or requiring them to be gleaned from consent orders.

In addition to the federal rules and guidance, Massachusetts enacted a data security regulation that became effective March 1, 2010. It applies to any entity that "receives, stores, maintains, processes, or otherwise has access to personal information [of a Massachusetts resident] in connection with the provision of goods or services or in connection with employment."[2]

Prior to the enactment of the cybersecurity regulation, many considered the Massachusetts regulation to be the most stringent state cybersecurity standard. The Massachusetts regulation may be considered to have initiated the movement away from the Safeguards Rule's deferential cybersecurity regulatory model and toward more prescriptive requirements. The cybersecurity regulation continues this trend.

The cybersecurity regulation does not include specific penalties for noncompliance, but the NYDFS has broad general authority relative to regulated entities under the Banking, Insurance and Financial Institutions laws of New York. For example, under the Banking Law, the NYDFS may, under certain circumstances, revoke the license or charter of a bank that has committed legal or regulatory violations.

For depository institutions, the FFIEC Handbook's information security booklet lists some of the regulatory expectations of the Safeguards Rule's cybersecurity requirements.

Another example: Section 44 of the Banking Law permits the NYDFS to assess fines for noncompliance with its regulations. These fines may be very steep — in some cases up to the lesser of $250,000 or 1% of the bank's assets per day of noncompliance. Finally, Section 44-a of the Banking Law permits the assessment of fines for failure to make required reports to the NYDFS. The fines may be even greater where there is a pattern of noncompliance.

What follows is review and comparison of the cybersecurity regulation to both the Massachusetts regulation and federal regulations and guidance as they relate to three key areas of security controls: multifactor authentication, encryption and security incident response. We have also noted where the FTC Safeguards Proposal (published for public comment April 4) marks a change in the federal approach on these issues.[3]

APPROACH TO MULTIFACTOR AUTHENTICATION

Since March 1, 2018, covered entities have been required to implement multifactor authentication as outlined in the cybersecurity regulation. Federal regulators have endorsed the use of multifactor authentication for several years. While Massachusetts generally requires secure user authentication protocols, the Massachusetts regulation does not require that the protocols employ multiple authentication factors.

FFIEC GUIDANCE

On Aug. 8, 2001, the FFIEC released its "Authentication in an Electronic Banking Environment" guidance. The 2001 FFIEC guidance noted that customer authentication is an "imperative" for banks engaging in electronic commerce in order to gain consumer trust in the then-nascent e-banking market and to prevent fraud.

Single-factor authentication tools, such as passwords and PINs, were then widely accepted as commercially reasonable for many electronic-banking activities even though hackers were more frequently undermining those measures. In recognition of that reality, the 2001 FFIEC guidance recommends that financial institutions also consider implementing multifactor authentication methods on "sensitive internal or high-value systems" to reduce their losses.

Four years later, on Oct. 12, 2005, the FFIEC revised its guidance in the "Authentication in an Internet Banking Environment" guidance. Accounts and transactions that relied solely on single-factor authentication were increasingly compromised by sophisticated cyberattacks.

Against this backdrop, the 2005 FFIEC guidance states that financial institutions with inadequate single-factor authentication should implement either multifactor authentication, layered security or other controls to fortify their defense against attacks involving access to consumer information or the external transfer of funds.

Specifically, the 2005 FFIEC guidance noted that "[t]he agencies consider single-factor authentication, as the only control mechanism, to be inadequate for high-risk transactions involving access to customer information or the movement of funds to other parties."

On June 28, 2011, the FFIEC issued additional guidance regarding cybersecurity titled "Supplement to Authentication in an Internet Banking Environment." Because experience has shown that hackers can circumvent virtually every authentication technique, the FFIEC expects that financial institutions not rely on any single control for authorizing high-risk transactions, but rather institute a layered system of security.

That is, businesses should use different controls at different points in a transaction process to reinforce the vulnerabilities of any one control. The FFIEC provides the following examples of effective controls that may be included in a layered security program, including many that are not based directly upon authentication:

- Fraud detection and monitoring systems that include consideration of customer history and behavior and enable a timely and effective institution response.
- Use of dual customer authorization through different access devices.
- Use of out-of-band verification for transactions.
- Internet protocol reputation-based tools to block connection to banking servers from IP addresses known or suspected to be associated with fraudulent activities.
- Policies and practices for addressing customer devices identified as potentially compromised and customers who may be facilitating fraud.
- Enhanced customer education to increase awareness of the fraud risk and effective techniques customers can use to mitigate risk.

The FFIEC expects that each layered cybersecurity program will enable the business to detect and respond to suspicious activity. It noted that the layered security program should also feature enhanced controls for system administrators to allow them to set up or change administrative access and system functions for business accounts.

In addition to layered security, the FFIEC recommends that institutions offer multifactor authentication to their business customers. It observes that online business transactions are both more frequent and also consist of higher-dollar expenditures than online consumer transactions and thus pose a "comparatively increased level of risk" — an increased risk that multifactor authentication can address.

MASSACHUSETTS' DATA SECURITY REGULATION

On March 1, 2010, Massachusetts' Office of Consumer Affairs and Business Regulation issued the Massachusetts regulation, which requires entities to employ "secure user authentication protocols" but does not impose any of the specific security solutions that the 2011 FFIEC guidance recommends.

Entities do not have to install these protocols if they can show the protocols are not "technically feasible." This defense may erode as technology and solutions become more accessible and affordable. The authentication protocols must provide for either a reasonably secure way to assign and select passwords for users, or use "unique identifier technologies, such as biometrics or token devices."

These authentication requirements operate on top of other measures, such as the reasonable monitoring of systems for unauthorized use of or access to personal information, encryption, and ongoing employee cybersecurity training.

However, the Massachusetts regulation does not require that institutions use multifactor authentication. Nor does it contemplate the FFIEC standard for layered security — that is, enhanced controls for system administrators to implement at different stages of a transaction.

NYDFS

Since Aug. 28, 2017, nonexempt covered entities in New York have been required to maintain a cybersecurity program designed to protect the "confidentiality, integrity and availability" of their information systems. One specific designation of the cybersecurity program is the use of defensive infrastructure. In conjunction with the cybersecurity program, nonexempt entities must also implement and maintain a written cybersecurity policy that addresses their "access controls and identity management."

> Federal regulators have endorsed the use of multifactor authentication for several years.

Since March 1, 2018, covered entities in New York have also been required to use effective controls to protect against certain unauthorized access to the nonpublic information they hold or the information systems they use. The NYDFS lists multifactor authentication as one such effective control option.

The NYDFS defines "multifactor authentication" as the verification of at least two of the following types of authentication factors: knowledge factors (e.g., passwords), possession factors (e.g., token or mobile phone text message) or inherence factors (e.g., biometrics). This structure largely follows the model established in 2001 by the FFIEC.

The cybersecurity regulation does not explicitly require multifactor authentication, except in the context of external access to the covered entity's internal network. In other contexts, it simply states that a company must use "effective controls," which may include multifactor authentication.

Even where multifactor authentication is required, the cybersecurity regulation permits the covered entity's chief information security officer to authorize the use of a "reasonably equivalent or more secure" alternative access control. This provision places the CISO in a new and precarious position. If multifactor authentication is not appropriate or feasible in a given situation, the CISO must now find another defensible solution and provide written approval for its use.

New York also has explicit requirements to vet the adequacy of multifactor authentication used by third-party service providers. To the extent applicable, covered entities must have policies and procedures that address the necessary due diligence and contractual protections required for evaluating a third-party service provider's use of multifactor authentication.

However, as noted on the NYDFS Cybersecurity FAQ webpage, the mandate for third-party service providers' use of multifactor authentication is based on the covered entity's risk assessment regarding the appropriate controls for third-party service providers.

FTC SAFEGUARDS RULE PROPOSAL

As in many areas of security controls, the FTC Safeguards Rule proposal would change the federal approach to cybersecurity regulation to incorporate more specific control requirements into the regulation.

> The Massachusetts regulation does not require that institutions use multifactor authentication.

For authentication, the proposal would require financial institutions to "implement multi-factor authentication for any individual accessing customer information."[4] In fact, the FTC notes that the revised authentication requirement is based on the requirement in Section 12 of the cybersecurity regulation.

The FTC Safeguards Proposal defines "multi-factor authentication" as "authentication through verification of at least two of the following types of authentication factors: Knowledge factors, such as a password; possession factors, such as a token; or inherence factors, such as biometric characteristics."

This change in approach by the FTC confirms the trend toward more specific control requirements and shows that regulators are looking to the issuances of other regulators in the formulation of new cybersecurity requirements.

ENCRYPTION

New York's encryption requirements go beyond existing requirements in the FFIEC Handbook, the Massachusetts regulation, and the Safeguards Rule, which do not directly address encryption. As with authentication, the FTC Safeguards Rule proposal looks to the cybersecurity regulation as a source and follows its more prescriptive approach.

FFIEC HANDBOOK

Under the FFIEC Handbook, management should implement the type and level of encryption commensurate with the sensitivity of the information. The FFIEC notes that encryption can be used "throughout a technological environment" including in operating systems, file systems, applications, and communication protocols. Encryption methods should be reviewed "periodically" to ensure that they keep up with evolving technology and defense standards.

The FFIEC also states that electronically stored passwords should be hashed (i.e., algorithmically transformed into a character string) or encrypted. Furthermore, any passwords should also be salted (i.e., a random string of data should be applied to each password) before hashed in order to create unique passwords for every user.

Finally, the FFIEC states that effective controls over the "generation, exchange, storage, use, and replacement of [cryptographic] keys" is "crucial" to the effective use of encryption.

MASSACHUSETTS DATA SECURITY REGULATION

In general, Massachusetts requires the encryption of personal information that is transmitted across public networks, transmitted wirelessly, or stored on laptops or other portable devices. Massachusetts defines the term "encrypted" as "the transformation of data into a form in which meaning cannot be assigned without the use of a confidential process or key."

Massachusetts acknowledges that the cost of commercial solutions adopted should be proportional to the risk exposure. Its regulation provides that a person must implement the prescribed security features, such as encryption, only to the extent "technically feasible."

The Office of Consumer Affairs and Business Regulation has defined its understanding of this exception narrowly in its website resource materials, finding "technically feasible" to mean that if there is a reasonable means through technology to accomplish a required result, then that reasonable means must be used.

NYDFS

Since Sept. 3, 2018, covered entities in New York have been required to encrypt nonpublic information that is either in transit over external networks or at rest. While the Massachusetts regulation provides an exception if encryption is not technically feasible, NYDFS requires that even if encryption is "infeasible," the covered entity's CISO must employ "effective alternative compensating controls" to protect nonpublic information.

Instead of enjoying an exception, the CISO of a New York covered entity bears the responsibility of determining that encryption is infeasible, finding alternative controls that may be used, assessing the effectiveness of the alternative controls, and annually assessing the feasibility of encryption and alternative controls.

New York's requirements for the encryption processes used by third-party service providers meet the same level of detail as other parts of the cybersecurity regulation. Covered entities must have pre-existing guidelines for the due diligence and contractual protections relating to the use of third-party service providers. In short, institutions must be able to evaluate whether the third-party service provider can match its own standards for the encryption of nonpublic information in transit and at rest.

FTC SAFEGUARDS RULE PROPOSAL

In the area of encryption, the FTC Safeguards Rule proposal again follows the approach of the cybersecurity regulation by generally requiring encryption of personal information in transit and at rest. The FTC notes that the encryption provisions are based on Section 15 of the cybersecurity regulation. Like the cybersecurity regulation, the FTC Safeguards Rule proposal permits the use of alternative controls if the use of encryption is infeasible, subject to review and approval by the CISO.

SECURITY INCIDENT RESPONSE

On March 29, 2005, the Office of the Comptroller of the Currency, the Board of Governors of the Federal Reserve System, the Federal Deposit Insurance Corp. and the Office of Thrift Supervision issued the Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice.

The response guidance states that an institution's response program should at least contain procedures for:

- Assessing the nature and scope of an incident and identifying what customer information systems and types of customer information have been accessed or misused.
- Notifying its primary federal regulator as soon as possible when the institution becomes aware of an incident involving unauthorized access to or use of sensitive customer information, as defined later in the final guidance.
- Immediately notifying law enforcement in situations involving federal criminal violations requiring immediate attention.
- Taking appropriate steps to contain and control the incident to prevent further unauthorized access to or use of customer information, such as by monitoring, freezing or closing affected accounts while preserving records and other evidence.
- Notifying customers when warranted.

The structure of this federal guidance differs from the general structure under the state laws. First, the institution is required to notify its primary regulator of all incidents, including "unauthorized access to or use of" sensitive customer information, but to notify affected customers only if certain criteria are met.

In contrast, under the state breach notice laws, the initial determination concerns whether individuals must be notified. Once that determination is made, the entity may under some state laws be required to notify one or more state agencies.[5]

Under the agencies' response guidance, the institution is required to notify a consumer of an incident of unauthorized access to their information when it determines, after a reasonable investigation, that misuse of the information "has occurred or is reasonably possible."

> As of September 3, 2018, a covered entity in New York must encrypt nonpublic information that is either in transit over external networks or at rest.

Many state laws require notice to affected state residents only where a security incident poses a requisite risk of harm to the state residents.[6] Other state laws require notice to impacted state residents regardless of whether an incident creates a risk of harm.[7]

MASSACHUSETTS DATA SECURITY REGULATION

The Massachusetts regulation, issued under the state's breach notice law, expands the scope of requirements relating to a security breach. Like the agencies' response guidance, the Massachusetts regulation contains requirements for notification to government agencies and affected individuals.

However, Massachusetts also appears to regard the security incident as an opportunity to examine the entity's information security program. In several cases involving security incidents, the Massachusetts attorney general's office cited the entity for failing to maintain an appropriate security program rather than for either the incident itself or failing to provide timely notice of it.[8]

Under the Massachusetts regulation, "every comprehensive information security program [must] ... [document] responsive actions taken in connection with any incident involving a breach of security, and [must include] mandatory post-incident review of events and actions taken, if any, to *make changes in business practices* relating to protection of personal information."[9]

Together with the requirement that an entity review the scope of security measures at least annually, the Massachusetts regulation requires an entity to continuously assess and invest in its security infrastructure (including the attendant policies and procedures) rather than allowing it to react in proportion to the harm it sustains.

NYDFS

Since Aug. 28, 2017, nonexempt covered entities in New York have been required to develop a written incident response plan, even if they have not yet experienced a security incident. The written plan requirement emphasizes that the NYDFS regards an entity's security information system to be as important as the personal information that the security system protects.

The incident response plan envisions both the response to and the recovery from any material cybersecurity event. The NYDFS requires written response plans to address:

- The internal processes for responding to a cybersecurity event.
- The goals of the incident response plan.
- The definition of clear roles, responsibilities and levels of decision-making authority.
- External and internal communications and information sharing.
- Identification of requirements for the remediation of any identified weaknesses in information systems and associated controls.
- Documentation and reporting regarding cybersecurity events and related incident response activities.
- The evaluation and revision, as needed, of the incident response plan following a cybersecurity event.

In addition, New York requires that the maintained systems include audit trails of information about cybersecurity events that have a reasonable likelihood of materially harming any material part of the normal operations.

The cybersecurity regulation also mandates that each covered entity notify the superintendent "as promptly as possible but in no event later than 72 hours" after the determination of certain "cybersecurity events," a term defined more broadly than a security breach under the breach notice statutes.

Such cybersecurity events are those that trigger notice obligations to "any government body, self-regulatory agency or any other supervisory body" and those that have "a reasonable likelihood of materially harming any material part of the normal operation(s) of the covered entity."

Prior to this deadline requirement, entities that experienced a cybersecurity breach had to comply with the various state data breach notification statutes. Those statutes mostly contain subjective notice deadlines, including "as soon as practicable" or "without unreasonable delay."

Because the requirements of the cybersecurity regulation apply to "nonpublic information," a term including both personal information and sensitive business information the "access or use of which, would cause a material adverse impact to the business, operations or security of the covered entity," the scope of the cybersecurity regulation's breach notification requirements is broader than state breach notice laws or the agencies' response guidance, which cover only personal information.

Notably, the NYDFS maintains that an attack on a covered entity may constitute a reportable cybersecurity event even if the attack is not successful. The NYDFS says there are many routine, unsuccessful attacks that do not merit the superintendent's attention, but the agency wants to be informed of them if they are sufficiently serious to be escalated within a company.

Reports of these failed attacks can serve as useful case studies to inform development of improved cybersecurity programs, according to the agency. The NYDFS states that it "does not intend to penalize" covered entities that in good faith do not report these incidents, though this statement does not preclude such an action.

Section 44(a) of the Banking Law permits the assessment of fines for failure to make required reports to the NYDFS. Fines can be steep, and they may be greater if the NYDFS discovers a pattern of noncompliance. A covered entity is well-advised to craft its security incident response plan in a manner that is mindful of the NYDFS' preference to be informed of all nonroutine attacks.

Finally, the cybersecurity regulation requires incident response plans to bring third-party service providers within their ambit. Covered entities must have pre-existing guidelines for conducting due diligence and enforcing contractual protections as they both relate to engaging a third-party service provider.

These guidelines include assuring adequate notice to the covered entity in the event of certain cybersecurity events. In particular, events that directly impact the covered entity's information systems or the nonpublic information it holds must trigger notice to the entity.

CONCLUSION

The NYDFS cybersecurity regulation reflects two important trends in cybersecurity regulation. First, cybersecurity programs are being held to higher standards that often demand the use of certain specific controls or defensible alternatives. This more prescriptive approach now affects the entities that do business in New York and may impact the general consensus, beyond New York, of what constitutes reasonable security.

Second, because federal legislation is increasingly difficult to enact and federal regulators are deemed less assertive nowadays, states are stepping in to fill the perceived gap.

Other states may follow the new model established by the NYDFS or seek to create their own models for cybersecurity regulation.

The FTC Safeguards Rule proposal shows that the cybersecurity regulation is influencing federal requirements. As security incidents and cybersecurity threats continue to headline the news, we anticipate increased pressure on government entities at both federal and state levels to take action.

NOTES

[1] Rules regarding the safeguarding of personal information by financial institutions were issued by several federal financial regulators under authority given by GLBA. The original versions of the Safeguards Rule were issued between 2000 and 2002, and the versions are substantively nearly identical. On April 4, the FTC issued a proposed revision to its version of the Safeguards Rule.

[2] 201 Mass. Code Regs. § 17.03(1), 17.02.

[3] While the FTC Safeguards Rule proposal addresses authentication and encryption, the proposed rule does not include security breach notification requirements, noting that "[a] federal standard under GLBA would be largely redundant because of state breach notification laws and because a requirement under the rule would have limited effect, because the commission cannot obtain civil penalties for violations of the rule." 84 Fed. Reg. 13158, 13171 at fn 123.

[4] 84 Fed. Reg. 13158, 13167 (Apr. 4, 2019).

[5] See, e.g., Cal. Civ. Code § 1798.82.

[6] For example, in New Jersey, disclosure of a breach is not required if the business or public entity establishes that "misuse of the information is not reasonably possible." N.J. Stat. Ann. § 56:8-163(a). In North Carolina, notification of the incident is not required if illegal use of the personal information has not occurred, illegal use is not reasonably likely to occur, or there is no material risk of harm to a consumer. N.C. Gen. Stat. § 75-61(14).

[7] See, e.g., N.Y. Gen. Bus. Law § 899-aa(2).

[8] See, e.g., Press Release, Maura Healey, Attorney General, Commonwealth of Massachusetts, Payment Processor to Pay $155,000 over Data Breach Affecting Thousands of Massachusetts Residents (Dec. 19, 2018), https://bit.ly/2JLcSJC; Press Release, Maura Healey, Attorney General, Commonwealth of Massachusetts, McLean Hospital to Implement New Security and Training Programs After Data Breach Exposed Sensitive Health Information (Dec. 19, 2018), https://bit.ly/2GTBTli; Press Release, Maura Healey, Attorney General, Commonwealth of Massachusetts, AG Healey Settles with Billing Company over Data Breach Impacting Children (Nov. 29, 2017), https://bit.ly/2wvGyBT.

[9] 201 Mass. Code Regs. § 17.03(2)(j) (emphasis added).

This article first appeared in the June 24, 2019, edition of Westlaw Journal Bank & Lender Liability.

ABOUT THE AUTHORS



(L-R) **Elizabeth E. McGinn**, a partner in the Washington and New York offices of **Buckley LLP**, assists clients in identifying, evaluating and managing risks associated with cybersecurity, internal privacy and information security practices. She can be reached at emcginn@buckleyfirm.com. **David Rivera** is a regulatory attorney in the firm's Washington office. He performs reviews related to fair lending risk assessments of mortgage servicing loss mitigation processes, responding to Federal Housing Finance Agency subpoenas, and preparing multi-state regulatory surveys and analyses for mortgage companies and banks. He can be reached at drivera@buckleyfirm.com. **James Shreve** is a partner with **Thompson Coburn LLP** in Chicago, where he chairs the firm's cybersecurity group. He serves as a trusted advisor to clients facing complex cybersecurity and privacy issues, particularly those in the country's most highly regulated industries. He can be reached at jshreve@thompsoncoburn.com.