NORTH CAROLINA BANKING INSTITUTE

Volume 22 | Issue 1 Article 14

3-1-2018

NYDFS Cybersecurity Regulations: A Blueprint for Uniform State Statute?

Sabrina Galli

Recommended Citation

Sabrina Galli, *NYDFS Cybersecurity Regulations: A Blueprint for Uniform State Statute?*, 22 N.C. Banking Inst. 235 (2018).
Available at: http://scholarship.law.unc.edu/ncbi/vol22/iss1/14

NYDFS Cybersecurity Regulations: A Blueprint for Uniform State Statute?

I. INTRODUCTION

One hundred forty-three million Americans, including five million North Carolinians,[1] were affected by the Equifax breach reported in September 2017.[2] The names, birthdates, social security numbers, and addresses of over half of the adult population were compromised.[3] Although so many Americans have been affected by this breach, consumers remain in the dark about any potential remedies against Equifax.[4] One year of free credit monitoring was the sole remedy offered to consumers, without taking into consideration the power of a social security number and the degree of harm that can be caused when such valuable information is in the wrong hands.[5] Because these breaches often cross multiple jurisdictions with different statutory schemes and conflicting case law, holding companies like Equifax accountable has become increasingly difficult.[6]

[1] N.C. ATTORNEY GEN.'S OFFICE, ATTORNEY GENERAL STEIN TAKES ACTION ON BEHALF OF FIVE MILLION NORTH CAROLINIANS IMPACTED BY EQUIFAX BREACH (Sept. 11, 2017), http://www.ncdoj.gov/News-and-Alerts/News-Releases-and-Advisories/Attorney-General-Stein-Takes-Action-on-Behalf-of-5.aspx.

[2] F. Paul Greene, *The Equifax Breach: Why this One is Different*, N.Y. L.J. (Sept. 13, 2017).

[3] *See id*. ("Among the personally identifiable information (PII) that was compromised was name, date of birth, address, and Social Security number. For some affected individuals, driver's license number and credit card number were also compromised.").

[4] *See* Tara Siegel Bernard & Stacy Cowley, *Equifax Hack Exposes Regulatory Gaps, Leaving Consumers Vulnerable*, N.Y. TIMES (Sept. 8, 2017), https://www.nytimes.com/2017/09/08/business/equifax.html?mcubz=0 ("The bureaus each have files on roughly 200 million Americans. And consumers have little choice, since banks and other companies hand over financial information and other data directly to the bureaus.").

[5] *See id*. ("The collateral damage can be devastating, and when you are talking about Social Security numbers the only expiration date a Social Security number has is yours.") (internal quotations omitted).

[6] *See* Josefa Velasquez, *Lawyers Say More Regulation is Likely to Follow Equifax Breach*, N.Y. L.J. (Sept. 20, 2017) (articulating how the Equifax breach potentially could lead to federal regulations as remedies are pursued and describing how states such as New York and Massachusetts have begun to file suits against Equifax).

New York has codified a solution to prevent such breaches that could pave the way for a uniform cybersecurity law.[7] In 2016, in the state of New York alone, there was a record-breaking 1,282 data breach notices affecting 1.6 million residents, 300% more New York residents than the year before.[8] Acknowledging that cybersecurity threats will continue to grow, the New York Attorney General released a report in 2014 stressing the importance of addressing such risks.[9] Between 2006 and 2013, there were nearly 5,000 individual data breaches, which exposed the personal information of 22.8 million New York residents.[10] In 2013, these data breaches cost New York businesses $1.37 billion.[11] In an attempt to keep up with the growth of technology and resulting increase of cybersecurity threats, New York was the first state to pass a non-breach oriented cybersecurity regulation to protect customer information.[12] The new data breach prevention regulations took effect March 1, 2017, pursuant to authority granted to the New York Department of Financial Services ("NYDFS"), and require all covered entities to take a preventative approach against the pervasive concerns of cybersecurity.[13]

This Note analyzes how NYDFS' new regulations place a tremendous amount of responsibility on financial institutions and shift the business strategy from a mindset of risk mitigation to one of regulatory compliance. This Note also analyzes how these regulations are likely to influence cybersecurity regulations across all major financial markets. This Note proceeds in six parts. Part II explains the legislative history of breach notification statutes and their failure to provide substantial protections against data breaches.[14] Part III describes who is

[7] N.Y. COMP. CODES R. & REGS. tit. 23, § 500.00 (2017).

[8] Justin Hemmings, *New York Attorney General Announces Record Number of Data Breach Notices in 2016*, ALSTON & BIRD, PRIVACY & DATA SECURITY BLOG (March 24, 2017), http://www.alstonprivacy.com/new-york-attorney-general-announces-record-number-data-breach-notices-2016/.

[9] *See* ERIC T. SCHNEIDERMAN, N. Y. ATTORNEY GEN.'S OFFICE, INFORMATION EXPOSED i (July 14, 2014), https://ag.ny.gov/pdfs/data_breach_report071414.pdf ("This report provides recommendations that individuals and organizations can implement to protect themselves from data loss. While the defensive measures we recommend for individuals and businesses can be helpful, the scope of the data breach problem detailed in this report demands a systemic response.").

[10] *Id.* at 1.

[11] *Id.*

[12] N.Y. COMP. CODES R. & REGS. tit. 23, § 500.00 (2017).

[13] *Id.*

[14] *See infra* Part II.

covered by the new data breach prevention regulations and what entities may be exempt.[15] Part IV examines best practices for compliance and potential methods for regulatory enforcement.[16] Part V calls for future uniform data breach prevention regulation.[17] Part VI concludes that the NYDFS regulations have the potential to be more effective than simple data breach notification policies and therefore a successful model for other states.[18]

II. THE FAILURE OF BREACH NOTIFICATION STATUTES

Governor Andrew Cuomo created the NYDFS as part of his budget in 2011, merging both the New York State Banking Department and the New York State Insurance Department.[19] NYDFS now encompasses the functions of both former departments, and through its statutory authority to respond to the needs of the financial industry, created the new cybersecurity requirements.[20] The new regulations, ("Breach Prevention Regulations"), were created to help guard against cybersecurity threats so that New Yorkers can keep their private information protected.[21] NYDFS' statutory authority to create these laws stems from section 102 of New York Financial Services Law,[22] allowing the department to use its financial expertise to impose regulations that both help consumers and are "responsive to the needs of the banking and insurance industries."[23] Before these new regulations were implemented, New York's cybersecurity legislation was very similar to other states in that the statutes were limited to notification of affected parties after a breach.[24] Under this statute, financial institutions must notify consumers

[15] *See infra* Part III.

[16] *See infra* Part IV.

[17] *See infra* Part V.

[18] *See infra* Part VI.

[19] N. Y. DEP'T OF FIN. SERV., NYDFS: HISTORY, http://www.dfs.ny.gov/about/history.htm (last visited Sept. 3, 2017).

[20] N.Y. FIN. SERV. L. § 102 (2017); N. Y. DEP'T OF FIN. SERV., *supra* note 19.

[21] Press Release, N.Y. Dep't of Fin. Serv., DFS Issues Updated Proposed Cybersecurity Regulation Protecting Consumers and Financial Institutions (Dec. 28, 2016) (on file with author).

[22] N.Y. COMP. CODES R. & REGS. tit. 23, Ch. I, Pt. 500, Refs & Annos (2017).

[23] N.Y. FIN. SERV. L. § 102; *see also* N.Y. COMP. CODES R. & REGS. tit. 23, ch. I, pt. 500, Refs & Annos (explaining that statutory authority is also found in sections 201 regarding policy-making, 202 and 301 establishing the power of the superintendent, 302 allowing the superintendent to create regulations, and 408 providing the power to impose civil penalties).

[24] N.Y. GEN. BUS. LAW § 899-aa (2012).

following the discovery or notification of a breach in which an unauthorized user gained access to a consumer's private information.[25]

Breach notification legislation is common across the United States but has not been successful as a preventative measure.[26] The purpose of New York's comprehensive cybersecurity regulations is "to promote the protection of customer information as well as the information technology systems of regulated entities."[27] Currently, forty-eight states have enacted data breach notification statutes, all of which focus on data that an organization has in its possession or otherwise owns or licenses.[28] These notification statutes require institutions to notify consumers and the state attorney general immediately after a security breach.[29] New York's breach notification statute requires:

> Any person or business which conducts business in New York state, and which owns or licenses computerized data which includes private information shall disclose any breach of the security of the system following discovery or notification of the breach in the security of the system to any resident of New York state whose private information was, or is reasonably believed to have been, acquired by a person without valid authorization.[30]

Although this statute remains in effect, the new breach prevention regulations require that covered entities implement programs to prevent breaches in addition to the prior notification requirement.[31]

[25] *Id.* § 899-aa(2).

[26] *See e.g.*, N.C. ATTORNEY GEN.'S OFFICE, SECURITY BREACH INFORMATION, http://www.ncdoj.gov/getdoc/c4549c4c-9894-4a61-b801-48171c01f566/Security-Breach-Information.aspx (providing examples of the 9.3 million North Carolinians that have been affected by security breaches, even with breach notification statutes in place) (last visited Jan. 31, 2018).

[27] N.Y. COMP. CODES R. & REGS. tit. 23, § 500.00.

[28] Greene, *supra* note 2.

[29] N.Y. GEN. BUS. LAW § 899-aa(1)(c)(2); *see also* David Thaw, *Data Breach (Regulatory) Effects*, 2015 CARDOZO L. REV. 151, 161-63 (arguing that breach notification must be paired with more stringent cybersecurity measures in order to be effective, specifically promoting a bifurcated notification system first to a federal agency and then potentially to the consumer).

[30] N.Y. GEN. BUS. LAW. § 899-aa.

[31] *Id.*

The uniformity of state breach notification statutes demonstrates the potential for uniformity of cybersecurity breach prevention regulations.[32] Almost all states, including North Carolina and California, have very similar breach notification statutes.[33] In North Carolina, a security breach is defined as "[a]n incident of unauthorized access to and acquisition of unencrypted and unredacted records or data containing personal information where illegal use of the personal information has occurred or is reasonably likely to occur or that creates a material risk of harm to a consumer."[34] This includes any form of unauthorized access, excluding actions of employees of the institutions in good faith for a lawful purpose.[35] North Carolina's statute also distinguishes between whether the information is owned by the business or an outside party.[36] If the company owns or licenses personal information that has been breached, "disclosure notification shall be made without unreasonable delay."[37] If the company does not own or license the information, the entity must provide immediate notification.[38] In California, the first state to enact a breach notification statute,[39] if the company owns the

[32] *See Security Breach Notification Laws*, NAT'L CONFERENCE OF STATE LEGISLATURES (Feb. 6, 2018), http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx ("Forty-eight states, the District of Columbia, Guam, Puerto Rico and the Virgin Islands have enacted legislation requiring private or governmental entities to notify individuals of security breaches of information involving personally identifiable information.").

[33] *Id*.

[34] N.C. GEN. STAT. § 75-61(14) (2016).

[35] *Id*. ("Good faith acquisition of personal information by an employee or agent of the business for a legitimate purpose is not a security breach, provided that the personal information is not used for a purpose other than a lawful purpose of the business and is not subject to further unauthorized disclosure.").

[36] *See id*. § 75-65 (explaining that if not owned by the business, notification of the breach must be relayed immediately versus without unreasonable delay).

[37] *See id*. ("The disclosure notification shall be made without unreasonable delay, consistent with the legitimate needs of law enforcement, as provided in subsection (c) of this section, and consistent with any measures necessary to determine sufficient contact information, determine the scope of the breach and restore the reasonable integrity, security, and confidentiality of the data system.").

[38] *See id*. § 75-65(b) ("Any business that maintains or possesses records or data containing personal information of residents of North Carolina that the business does not own or license, or any business that conducts business in North Carolina that maintains or possesses records or data containing personal information that the business does not own or license shall notify the owner or licensee of the information of any security breach immediately following discovery of the breach, consistent with the legitimate needs of law enforcement as provided in subsection (c) of this section.").

[39] KAMALA D. HARRIS, CAL. DEP'T OF JUSTICE, CALIFORNIA DATA BREACH REPORT 1 (Feb. 2016) [hereinafter CA DATA BREACH REPORT], https://oag.ca.gov/sites/all/files/agweb/pdfs/dbr/2016-data-breach-report.pdf.

information, "[t]he disclosure shall be made in the most expedient time possible and without unreasonable delay."[40] If the company does not own the information, it "shall notify the owner or licensee of the information of any breach of the security of the data immediately following discovery . . . ."[41] The North Carolina statute indicates that notice should include a description of the incident, "the type of personal information that was subject to the unauthorized access and acquisition," a description of the acts the business took to protect that information, a telephone number for the business, the Federal Trade Commission ("FTC"), and the North Carolina's Attorney General's Office, as well as advice to remain vigilant.[42] Under California Civil Code § 1798.29(d)(1), "[t]he security breach notification shall be written in plain language, shall be titled 'Notice of Data Breach,' and shall present the information described in paragraph (2) under the following headings: 'What Happened,' 'What Information Was Involved,' 'What We Are Doing,' 'What You Can Do,' and 'For More Information.'"[43]

When these statutes were created in the early 2000s,[44] data breaches were only beginning to occur.[45] Since implementation of these statutes, data breaches have become a more serious problem.[46] According to North Carolina Attorney General Josh Stein, over 9.3 million North Carolinians have been subjected to data breaches since 2005.[47] California's Attorney General released a similar report in 2016 showing that in 2012, 131 breaches placed 2.6 million records of Californians at risk,[48] in contrast to 24 million records in 2015.[49] In California's financial sector, breaches resulting from insider error and

[40] CAL. CIV. CODE § 1798.29(a) (2016).

[41] *Id.*

[42] N.C. GEN. STAT. § 75-65(d) (2016).

[43] CAL. CIV. CODE § 1798.29(d)(1).

[44] CAL. CIV. CODE § 1798.29; N.C. GEN. STAT. § 75-65; N.Y. GEN. BUS. LAW. § 899-aa (2012).

[45] *See* Press Release, Michael F. Easley, N.C. Governor's Office, Gov. Easley Signs Identity Theft Protections Act (Sept. 21, 2005) (on file with author) (explaining that North Carolina's breach notification law was implemented to protect the 300,000 North Carolinians that were victims of data breaches each year prior to 2005).

[46] *See* N.C. ATTORNEY GEN.'S OFFICE, *supra* note 26 (demonstrating the rise of security breaches in North Carolina since 2005); *see also* CA DATA BREACH REPORT, *supra* note 39 (showing the rise of security breaches in California and the main causes of such breaches).

[47] N.C. ATTORNEY GEN.'S OFFICE, *supra* note 26.

[48] CA DATA BREACH REPORT, *supra* note 39, at iii.

[49] CA DATA BREACH REPORT, *supra* note 39, at iii.

abuse of access were much more prevalent than in other sectors.[50] At the end of report, the California Attorney General provided recommendations moving forward – such as creating multi-factor authentication and strong encryption – that mirror the new breach prevention regulations.[51]

Before the implementation of the new regulations, New York's Attorney General had similar, more proactive recommendations in his 2014 report.[52] These recommendations include minimizing the collection of data, creating an encrypted information security plan, and offering mitigation services to consumers.[53] In comparison to the breach notification statutes, NYDFS' breach prevention regulations instead require notice to the NYDFS superintendent within seventy-two hours if there is "a reasonable likelihood of materially harming any material part of the normal operation(s) of the Covered Entity."[54] Just as California was the first state to impose data breach notification legislation,[55] acting as the catalyst for national uniformity, New York could be the flagship for more stringent, uniform data breach prevention regulations.[56]

III. NYDFS DATA PREVENTION REGULATIONS: WHO'S IN AND WHO'S OUT

Under the NYDFS regulations, financial institutions are "covered entities" subject to the regulation if they qualify as "any Person operating under or required to operate under a license, registration, charter, certificate, permit, accreditation or similar authorization under the [New York] Banking Law, the Insurance Law or the Financial Services Law."[57] The regulation's definition of person covers both individuals and non-

[50] CA DATA BREACH REPORT, *supra* note 39, at iv.

[51] CA DATA BREACH REPORT, *supra* note 39, at 27.

[52] *See* SCHNEIDERMAN, *supra* note 9, at 2 (recommending five steps for organizations to prevent against unauthorized disclosures of information).

[53] *See* SCHNEIDERMAN, *supra* note 9, at 2 (recommending five steps for organizations to prevent against unauthorized disclosures of information).

[54] N.Y. COMP. CODES R. & REGS. tit. 23, § 500.17(a)(2) (2017).

[55] CA DATA BREACH REPORT, *supra* note 39.

[56] *See* Richard Hill, *N.Y. Rule Could Be Model for Cyber-Collaboration*, 108 Banking Rep. (BNA) No. 458 (March 23, 2017) (discussing whether New York's regulations could be a model for other similar regulations across the nation).

[57] N.Y. COMP. CODES R. & REGS. tit. 23, § 500.01(c).

governmental entities, including financial institutions.[58] New York branches of out-of-state domestic banks are not required, but instead strongly encouraged, to comply with the regulations.[59] New York covered institutions include nearly all major financial institutions incorporated or headquartered in New York, such as JP Morgan Chase Co., Signature Bank, Deutsche Bank Trust Company Americas, Goldman Sachs Bank USA, The Bank of New York Mellon, and New York Community Bank.[60]

Although not included in the original proposed rule, three compliance exemptions were included in the final regulation.[61] Any institution that fits the criteria for one of the exemptions must file a notice of exemption with the superintendent within thirty days of determination that an exemption applies.[62] The first set of exemptions is aimed at small businesses: entities with fewer than ten employees or less than $5 million in gross annual revenue from New York business operations or less than $10 million in year-end total assets are exempt from the requirements of implementing vulnerability assessments, audit trail, application security, designated cybersecurity personnel and Chief Information Security Officer, multi-factor authentication, training and monitoring, encryption of non-public information, and an incident response plan.[63]

This exemption, created to help small institutions that may not be able to cost effectively comply with the regulations, will undoubtedly have negative effects as well.[64] Although utilizing available resources is important for any entity, consistency in as many requirements as possible

[58] *Id.* § 500.01(i) ("*Person* means any individual or any non-governmental entity, including but not limited to any nongovernmental partnership, corporation, branch, agency or association.").

[59] N.Y. DEP'T OF FIN. SERV., FREQUENTLY ASKED QUESTIONS REGARDING 23 NYCRR 500 (2017), http://www.dfs.ny.gov/about/cybersecurity_faqs.htm.

[60] MARIA T. VULLO, N.Y. DEP'T OF FIN. SERV., 2016 ANNUAL REPORT 1, 30, 31, 35 (2015), http://www.dfs.ny.gov/reportpub/annual/dfs_annualrpt_2016.pdf.

[61] Joseph P. Vitale, *NYDFS' Revision of Proposed Cybersecurity Regulation for Financial Services Companies*, HARV. L. SCH. F. ON CORP. GOVERNANCE & FIN. REG. (Jan. 10, 2017), https://corpgov.law.harvard.edu/2017/01/10/nydfs-reversal-of-its-proposed-cybersec
urity-regulation-for-financial-services-companies/.

[62] N.Y. COMP. CODES R. & REGS. tit. 23, § 500.19(e).

[63] N.Y. COMP. CODES R. & REGS. tit. 23, § 500.19.

[64] *See Wall Street's Fourth Quarter Earnings*, N.Y. TIMES (Jan. 20, 2016), https:// www.nytimes.com/interactive/2015/04/13/business/dealbook/13db-wall-street-earnings.html?mcubz=0 (highlighting fourth quarter earnings for many of New York's covered entities).

will help lighten the burden for all.[65] Exempt companies still have to implement a cybersecurity policy and program, as well as provide notification to the superintendent if a cybersecurity event occurs; however, they do not need to create an incident response plan.[66] The incident response plan is "designed to promptly respond to, and recover from, any Cybersecurity Event materially affecting the confidentiality, integrity or availability of the Covered Entity's Information Systems or the continuing functionality of any aspect of the Covered Entity's business or operations."[67] While larger institutions may be spending $500 million on cybersecurity efforts each year,[68] smaller institutions with less accessible resources are more susceptible to threats, making an incident response plan extremely helpful in remaining proactive.[69] The response plan requires the entity to detail valuable information such as "internal processes for responding to a Cybersecurity Event," "the definition of clear roles, responsibilities and levels of decision-making authority," and "identification of requirements for the remediation of any identified weaknesses in Information Systems and associated controls."[70] Because the gravity of the compromised information remains the same, regardless of the size of the entity,[71] and because the incident response plan does not, on its face, require any monetary resources,[72] entities exempt under § 500.19(a) should still be required to create the incident response plan.

[65] DANIAL ILAN ET AL., CLEARY GOTTLIEB STEEN & HAMILTON, CLIENT ALERT: NYDFS CYBERSECURITY REGULATIONS TAKE EFFECT 5 (Aug. 21, 2017), https://www.clearygottlieb.com/~/media/cgsh/files/2017/publications/alert-memos/nydfs-cybersecurity-regulations-take-effect-8-21-17.pdf.

[66] N.Y. COMP. CODES R. & REGS. tit. 23, § 500.19(a); Thaw, *supra* note 24, at 4.

[67] N.Y. COMP. CODES R. & REGS. tit. 23, § 500.16(a).

[68] Hill, *supra* note 56.

[69] *See* Daniel R. Stoller, *Small Businesses Need Big Help in Cyberthreat Information Sharing*, 16 Privacy & Security Law Rep. (BNA) No. 44 (Nov. 6, 2017) ("Small businesses are struggling to leverage limited resources to effectively contribute to U.S. public-private cyberthreat information programs . . . These smaller companies can offer valuable insight into everyday cybersecurity threat indicators that could slip through the cracks . . . .").

[70] N.Y. COMP. CODES R. & REGS. tit. 23, § 500.16.

[71] *See* Stoller, *supra* note 69 (explaining how smaller companies are valuable in sharing information about security breaches).

[72] N.Y. COMP. CODES R. & REGS. tit. 23, § 500.16.

A second exemption applies to those who are already included under a covered entity's cybersecurity program, such as an employer.[73] Covered entities that do not "directly or indirectly operate, maintain, utilize or control any Information Systems" or "directly or indirectly control, own, access, generate, receive or possess Nonpublic Information" only have to comply with the risk assessment, third-party service-provider policy, the limitations on data retention, and breach notification requirements.[74]

The last exemption applies to covered entities under Article 70 of the Insurance Law that do not have access to non-public information "other than information relating to its corporate parent company (or Affiliates)."[75] Entities exempt under this provision are subject to the same compliance requirements as those mentioned above.[76]

IV. REQUIREMENTS, ENFORCEMENT, AND BEST PRACTICES FOR COMPLIANCE WITH BREACH PREVENTION REGULATIONS

A. *Initial Drafting of the Regulations and Concerns of the Public*

Before issuing its final rule, NYDFS first had a forty-five day comment period and then instituted a thirty-day final comment period after the updated draft was published on December 28, 2016.[77] Original comments about the regulation critiqued its broad provisions, many of which then became narrowly tailored in the second draft.[78] One of the most significant changes was the definition on nonpublic information, which was first described as any business-related information or information:

[73] *Id.* § 500.19(b) ("An employee, agent, representative or designee of a Covered Entity . . . need not develop its own cybersecurity program to the extent that the employee, agent, representative or designee is covered by the cybersecurity program of the Covered Entity.").

[74] *Id.* § 500.19(c); STEVEN CHABINSKY ET AL., WHITE & CASE LLP, CLIENT ALERT: NYDFS CYBERSECURITY REGULATIONS COMPLIANCE GUIDE: APPLICABLE EXEMPTIONS AND PENALTIES 4 (March 2017), https://www.whitecase.com/sites/whitecase/files/files/download/publications/nydfs-cybersecurity-regulations-ver392017.pdf.

[75] N.Y. COMP. CODES R. & REGS. tit. 23, § 500.19(d).

[76] *Id.*

[77] N.Y. DEP'T FIN. SERV., *supra* note 19.

[78] Vitale, *supra* note 61; *see also* F. Paul Greene, *Final DFS Cybersecurity Regulations: Questions of Scope and Effect Linger*, N.Y. L. J. (Feb. 28, 2017) (discussing how the new regulations differ from past legislation and which original provisions of the legislation did not become part of the final regulation).

> that an individual provides to a Covered Entity in connection with the seeking or obtaining of any financial product or service from the Covered Entity, or is about an individual resulting from a transaction involving a financial product or service between a Covered Entity and an individual, or a Covered Entity otherwise obtains about an individual in connection with providing a financial product or service to that individual.[79]

Although the finalized regulation still includes business-related information,[80] it specifies that nonpublic information includes:

> Any information concerning an individual which because of name, number, personal mark, or other identifier can be used to identify such individual, in combination with any one or more of the following data elements: (i) social security number, (ii) drivers' license number or non-driver identification card number, (iii) account number, credit or debit card number, (iv) any security code, access code or password that would permit access to an individual's financial account, or (v) biometric records.[81]

By specifying what kinds of information may be jeopardized in a breach, the regulations guarantee that entities cannot hide behind or be confused by the broad language of information "in connection with the seeking or obtaining of any financial product or service."[82] Those changes were made in response to comments that the original language "was overbroad, unclear or unnecessarily inconsistent with other existing standards."[83] This provision also mirrors the definition used in New York's breach notification statute, with the exception of "biometric measures" which may have been added to incorporate the growth of technology.[84]

[79] Vitale, *supra* note 61.

[80] N.Y. COMP. CODES R. & REGS. tit. 23, § 500.01(g)(1).

[81] *Id.* § 500.01(g)(2).

[82] Vitale, *supra* note 61.

[83] Vitale, *supra* note 61.

[84] N.Y. GEN. BUS. LAW § 899-aa(1)(b) (2012).

Although the definition of "nonpublic information" received a great deal of criticism during the comment period, another cause for concern was the requirement that each covered entity designate a qualified individual as a Chief Information Security Officer ("CISO").[85] Commenters expressed specific concerns that institutions would have to hire or appoint someone to that position as his or her sole job.[86] The final regulation specifies, however, that the CISO can be employed by the institution itself, a third party, or an affiliate.[87] If the institution selects one of the latter two options, it must ensure its own compliance with the regulations and require the third party to create its own cybersecurity program.[88] The CISO maintains a great deal of responsibility because if a third party fails to uphold the cybersecurity program, the covered entity will still be held liable.[89] The entity is trusting the third party with access to nonpublic information and is therefore held accountable.[90] Perhaps sharing part of the public concern, third parties – such as insurance companies and law firms – will be incentivized to comply with the regulations so that they are not the cause of a client's breach.[91] In order to maintain their business with the institutions, third parties will be obligated to comply with many of the regulations, such as using encrypted information and limiting user privileges on systems with nonpublic information.[92]

B. Enforcement of the Data Breach Prevention Regulations

The NYDFS superintendent is charged with enforcement of the regulation.[93] The superintendent's authority includes the ability to "impose fines or revoke an entity's license for noncompliance and potentially even hold personally liable the Board member or officer who

[85] N.Y. COMP. CODES R. & REGS. tit. 23, § 500.04; Vitale, *supra* note 61.

[86] Vitale, *supra* note 61.

[87] N.Y. COMP. CODES R. & REGS. tit. 23, § 500.04.

[88] *Id.* § 500.04(a)(2).

[89] *Id.* § 500.11.

[90] *Id.* §§ 500.11, 500.20.

[91] Barry R. Temkin, *New Cybersecurity Regulations: Impact on Representing Financial Institutions*, N.Y. L. J. (Dec. 15, 2016).

[92] *Id.*; *see also* Andrew M. Reidy & Joseph M. Saka, *New DFS Cybersecurity Regulations are Here: Will Your Insurance Protect You?*, N.Y. L. J. (June 5, 2017) (explaining how covered entities will have to alter their insurance policies to limit liability from third-parties).

[93] N.Y. COMP. CODES R. & REGS. tit. 23, § 500.20.

signed the annual certification."[94] If a partly false certification is filed, "a certifying officer whose Covered Entity is subsequently found to be non-compliant could potentially incur personal civil liability."[95] The regulations do not clearly emphasize what kind of public remedy is available, but New York statute allows the attorney general to file suit if a person or business fails to notify a consumer of a data breach.[96] In those cases, the court can award damages for actual costs and losses incurred by the consumer.[97] If failure to comply with the breach notification requirement was done knowingly or recklessly, the court may impose a civil penalty between $5,000 and $150,000.[98]

C. Requirements for Covered Entities and Best Practices for Compliance

The regulations set specific deadlines for compliance: August 28, 2017, February 15, 2018, March 1, 2018, September 3, 2018, and March 1, 2019.[99] By August 28, 2017, covered entities were required to: (1) designate a Chief Information Security Officer, (2) implement a cybersecurity program, (3) implement a cybersecurity policy that must be approved by board of directors or a senior officer, (4) limit user privileges on systems with access to nonpublic information, (5) designate qualified cybersecurity personnel to oversee cybersecurity functions, and (6) implement a written incident response plan in the event of a data security

[94] *Id.* § 500.20 ("This regulation will be enforced by the superintendent pursuant to, and is not intended to limit, the superintendent's authority under any applicable laws."); CHRISTOPHER LAVIGNE, SHEARMAN & STERLING LLP, NEW YORK STATE CYBERSECURITY REGULATIONS: FIRST MILESTONE IN SIGHT, WHAT IS NEXT ON THE HORIZON? (Aug. 22, 2017), http://www.shearman.com/en/newsinsights/publications/2017/08/nystate-cybersecurity-regulations.

[95] Michael Krimminger, *New York Cybersecurity Regulations for Financial Institutions Enter into Effect*, HARV. L. SCH. F. ON CORP. GOVERNANCE & FIN. REG. (March 25, 2017), https://corpgov.law.harvard.edu/?s=New+York+Cybersecurity+regulations+for+financial+institutions+enter+into+effect.

[96] N.Y. GEN. BUS. LAW. § 899-aa(6)(a) (2012).

[97] *Id.*

[98] *Id.*

[99] Joseph D. Simon & Elizabeth A. Murphy, *Cybersecurity Regulation for Financial Services Companies: New York State Leads the Way*, 30 J. TAX'N F. INST. 27 (2017); *see also* LAVIGNE, *supra* note 94 (highlighting ten steps for financial institutions to take to ensure they meet the February 15, 2018 deadline).

breach.[100] More recently, entities were required to submit a certificate of compliance to NYDFS by February 15, 2018.[101] Although September 3, 2018 marks the end of the eighteen-month transition period, entities have until March 1, 2019 to ensure third parties are covered under the regulations.

An initial compliance step is for a covered entity to determine what policies and procedures are already in place.[102] For example, entities should already have a procedure for providing notice of a cybersecurity event due to the breach notification requirements set forth in the data breach notification statute.[103] Institutions will only have to adjust that requirement by ensuring notification to the NYDFS superintendent within seventy-two hours.[104]

Next, entities must select a Chief Information Security Officer ("CISO") who is responsible for both the cybersecurity program and the policy.[105] The entity must determine whether the CISO will be hired internally or externally, keeping in mind that a covered entity can use an employee of an affiliate as the entity's CISO or a third-party service provider.[106] As the role of CISO develops, entities should create a line of command to the CISO and adjust responsibilities accordingly.[107] The CISO will be responsible for providing written, annual reports to the entity's board of directors, as well as for implementing and overseeing both the program and the policy.[108] Due to the tremendous responsibility of the CISO, it may be unwise for a company to give the title to an employee or senior officer who already plays a very significant role in the company.[109] Entities will also need to consider how consequences

[100] N.Y. COMP. CODES R. & REGS. tit. 23, § 500.22 (2017); Craig Newman & Kade Olsen, *Deadline to Meet DFS Cyber Regulation Is Monday*, JDSUPRA (August 24, 2017), http://www.jdsupra.com/legalnews/deadline-to-meet-dfs-cyber-regulation-95014/.

[101] *Id.* § 500.17(b).

[102] *See* LAVIGNE, *supra* note 94 (advising institutions to catalogue all existing programs, policies, and procedures related to cybersecurity).

[103] N.Y. GEN. BUS. LAW § 899-aa (2012).

[104] N.Y. COMP. CODES R. & REGS. tit. 23, § 500.17.

[105] *Id.* § 500.04(a).

[106] N.Y. DEP'T FIN. SERV., *supra* note 59.

[107] *Cybersecurity Requirements for Financial Services Companies*, ERNST & YOUNG 5 (Feb. 2017), http://www.ey.com/Publication/vwLUAssets/EY-cybersecurity-requirements-for-financial-services-companies/$FILE/EY-cybersecurity-requirements-for-financial-services-companies.pdf.

[108] *Id.*

[109] *See id.* ("Special attention should be paid to the independence of the CISO. Firms may need to revise roles and responsibilities across the first and second lines of defense.").

of non-compliance may play into who obtains those roles.[110] Penalties for non-compliance, under the superintendent's authority, include issuing a consent order or imposing civil damages.[111] To outsource the position, an entity may choose to designate a CISO from an affiliate entity.[112] Although the affiliate is not a third-party provider, the covered entity still has full responsibility for ensuring that the CISO complies with all of the regulations.[113] If the CISO chosen is a third party, then the covered entity has to implement specific policies to ensure the security of information held within that third party.[114] The entity will also have to designate a senior personnel member to oversee the third party and its compliance with the regulations.[115]

Covered entities then need to implement a cybersecurity program to protect information systems,[116] a cybersecurity policy establishing procedures to protect information stored on such systems,[117] and an incident response plan.[118] Institutions also need to ensure that access privileges are limited to protect information systems and nonpublic information.[119] The cybersecurity program must be able to identify any risks and consequently protect information by detecting and responding to attacks, recovering and restoring after attacks, and reporting according to the law.[120] It must include procedures for how the institution will test

[110] *See* N.Y. COMP. CODES R. & REGS. tit. 23, § 500.04 (2017) (detailing the CISO's responsibility to enforce the regulations and report to the entity's board of directors on both compliance and cybersecurity risks).

[111] CHABINSKY, *supra* note 74, at 4.

[112] N.Y. DEP'T FIN. SERV., *supra* note 59.

[113] N.Y. DEP'T FIN. SERV., *supra* note 59.

[114] *See* N.Y. COMP. CODES R. & REGS. tit. 23, § 500.11(a) ("Each Covered Entity shall implement written policies and procedures designed to ensure the security of Information Systems and Nonpublic Information that are accessible to, or held by, Third Party Service Providers.").

[115] *Id*. § 500.04(a)(2).

[116] *Id*. § 500.02(a).

[117] *Id*. § 500.03.

[118] *Id*. § 500.16(a) ("As part of its cybersecurity program, each Covered Entity shall establish a written incident response plan designed to promptly respond to, and recover from, any Cybersecurity Event materially affecting the confidentiality, integrity or availability of the Covered Entity's Information Systems or the continuing functionality of any aspect of the Covered Entity's business or operations.").

[119] *Id*. § 500.07 ("As part of its cybersecurity program, based on the Covered Entity's Risk Assessment each Covered Entity shall limit user access privileges to Information Systems that provide access to Nonpublic Information and shall periodically review such access privileges.").

[120] *Id*. § 500.02.

the security of applications related to its business practices.[121] As mentioned above, covered entities have until September 3, 2018 to fully build their cybersecurity program, providing room for adjustments as time passes.[122] With the growth of technology, institutions will have to take into account applications used both in-house and externally.[123]

Covered entities are also required to conduct annual penetration testing,[124] bi-annual vulnerability assessments,[125] and implement multi-factor authentication[126] by March 1, 2018.[127] September 3, 2017 was the deadline for covered entities to secure their cybersecurity programs and maintain audit trails.[128] Penetration testing requires the company to attempt infiltration of its databases and controls, examining ways a potential cybersecurity breach could occur.[129] While penetration testing essentially simulates a breach, the bi-annual vulnerability assessments require that institutions evaluate their resources and the effectiveness of their cybersecurity programs.[130] The required audit trails fall into two separate categories: (1) records that would allow the institution to reconstruct material transactions, which must be maintained for at least three to five years, and (2) records that will help the institution detect and respond to breaches, which must be kept for at least three years.[131]

[121] *Id.* § 500.02(b)(1); ERNST & YOUNG, *supra* note 106, at 6.

[122] Simon, *supra* note 99; LAVIGNE, *supra* note 94.

[123] N.Y. COMP. CODES R. & REGS. tit. 23, § 500.08; ERNST & YOUNG, *supra* note 106, at 6.

[124] N.Y. COMP. CODES R. & REGS. tit. 23, § 500.05(a) ("Covered Entities shall conduct annual Penetration Testing of the Covered Entity's Information Systems determined each given year based on relevant identified risks in accordance with the Risk Assessment.").

[125] *Id.* § 500.05(b) ("Covered Entities shall conduct . . . bi-annual vulnerability assessments, including any systematic scans or reviews of Information Systems reasonably designed to identify publicly known cybersecurity vulnerabilities in the Covered Entity's Information Systems based on the Risk Assessment.").

[126] *Id.* § 500.12 ("Multi-Factor Authentication shall be utilized for any individual accessing the Covered Entity's internal networks from an external network, unless the Covered Entity's CISO has approved in writing the use of reasonably equivalent or more secure access controls.").

[127] LAVIGNE, *supra* note 94.

[128] N.Y. COMP. CODES R. & REGS. tit. 23, § 500.06.

[129] *Id.* § 500.01(h) ("Penetration Testing means a test methodology in which assessors attempt to circumvent or defeat the security features of an Information System by attempting penetration of databases or controls from outside or inside the Covered Entity's Information Systems.").

[130] *Id.* § 500.05(b).

[131] *Id.* § 500.06.

Of these requirements, entities may differ the most in determining the depth of the multi-factor authentication. For consumers, passwords are becoming less effective in maintaining security, and the strength of a password is useless if the company's security measures are lacking.[132] However, in determining the steps for multi-factor authentication, entities must decide how many steps to require without losing consumer efficiency.[133] Under the regulation, entities must require at least two of three different types of authentication factors: "(1) knowledge factors, such as a password; or (2) possession factors, such as a token or text message on a mobile phone; or (3) inherence factors, such as a biometric characteristic."[134] These factors mirror the requirements set forth by the Payment Card Security Standards, which dictate that two independent factors must be used.[135] In determining which factors to apply, entities will have to balance maintaining security without dissuading consumers through the use of an over burdensome process.[136] Entities can best ensure that they are effectively implementing the factors by remaining up-to-date on what technology can support, such as fingerprint verification.[137]

Although many of the initial compliance requirements have already been implemented by financial institutions, covered entities have until September 3, 2018, to fully transition and implement its

[132] *See* Fola Akinnibi, *Payment Card Security Standards Body Updates Rules*, LAW360 (Apr. 28, 2016) https://www.law360.com/articles/790240/payment-card-security-standards-body-updates-rules (discussing how the Payment Card Industry's Security Standards Council now requires multi-factor authentication on all networks, not just untrusted ones); *see also* DELOITTE, ADDRESSING CYBER THREATS MULTI-FACTOR AUTHENTICATION FOR PRIVILEGED USER ACCOUNTS 4 (2015), https://www2.deloitte.com/content/dam/Deloitte/us/Documents/public-sector/us-federal-cyber-mfa-pov.pdf [hereinafter DELOITTE] ("Unfortunately, many privileged user accounts are still today protected with weak credentials, often only username/password, leaving systems and applications more vulnerable to attack.").

[133] *See* DELOITTE, *supra* note 133, at 5 (warning institutions about potential user convenience frustrations, particularly if too many steps are required).

[134] N.Y. COMP. CODES R. & REGS. tit. 23, § 500.01(f) (2017).

[135] PCI SECURITY STANDARDS COUNCIL, GUIDANCE FOR MULTI-FACTOR AUTHENTICATION (Feb. 2017), https://www.pcisecuritystandards.org/pdfs/Multi-Factor-Authentication-Guidance-v1.pdf.

[136] *See* DELOITTE, *supra* note 133, at 5 ("To maximize effectiveness, multi-factor technology must be mandatory for the entire population. This will reduce user convenience somewhat; for instance, if an authentication token is lost, damaged or stolen it must be replaced before the user can access the systems again.").

[137] *See* DELOITTE, *supra* note 133, at 5 ("Agencies should leverage the guidance and support offered by OMB as part of the Cybersecurity Sprint and work with experienced technical resources to evaluate their environments and pursue PIV implementation across the enterprise for assets that can support it.").

cybersecurity program.[138] Therefore, best practices for implementation are still highly relevant to adjust any procedures that may prove to be ineffective.[139] Other states considering cybersecurity regulations may learn how to fashion the most effective regulation based on the issues surfaced by the New York regulations.[140] Because these regulations already mirror a great deal of the federal law requirements, as detailed below, similar regulations could likely be successful in other states.[141] Many institutions already have a cybersecurity officer and written policies,[142] providing an insight into which kinds of policies are most successful.

V. FUTURE UNIFORM STATE REGULATION

NYDFS' breach prevention regulations, combined with previously established federal laws and standards, pave the way for uniform state regulation.[143] Recognizing the concern financial institutions have about meeting both federal and state regulations, the NYDFS' regulations overlap with many portions of the Gramm-Leach-Bliley Act (GLBA) and the subsequent Federal Trade Commission's ("FTC") Safeguards Rule.[144] The GLBA prohibits financial institutions from disclosing nonpublic personal information to any third parties without first notifying the consumer.[145] The consumer must also be given the opportunity to object to disclosure and provided details on how to

[138] Simon, *supra* note 99; LAVIGNE, *supra* note 94.

[139] Simon, *supra* note 99; LAVIGNE, *supra* note 94.

[140] Hill, *supra* note 56.

[141] *See* Hill, *supra* note 56 ("The final rules, which went into effect March 1, still duplicate some existing requirements, but lawyers, industry groups and others praised the department for at least considering the burdens that come with regulatory overlap.").

[142] *See* Hill, *supra* note 56 ("[M]ost regulators require entities to have a senior-level cyber point-person, but will use different nomenclature to describe them. Other common themes include requiring written policies and procedures, mandating internal and external risk- assessments . . . .").

[143] *See* Hill, *supra* note 56 (discussing the increase in federal cybersecurity guidance and the possibility of the NYDFS regulations establishing uniform cybersecurity standards).

[144] *See* 16 C.F.R. § 314 (2017) (creating standards for all financial institutions under the Federal Trade Commission regarding the safeguarding of customer information).

[145] 15 U.S.C. § 6802(a) (2016) ("Except as otherwise provided in this sub-chapter, a financial institution may not, directly or through any affiliate, disclose to a nonaffiliated third party any nonpublic personal information, unless such financial institution provides or has provided to the consumer a notice that complies with section 503.").

exercise nondisclosure.[146] The Safeguards Rule, a requirement of the GLBA, applies to all institutions under the FTC's jurisdiction and "sets forth standards for developing, implementing, and maintaining reasonable administrative, technical, and physical safeguards to protect the security, confidentiality, and integrity of customer information."[147] The purpose of the Safeguards Rule is to secure customer confidentiality and to protect against cybersecurity threats or unauthorized access.[148]

NYDFS' breach prevention regulations maintain those objectives[149] while requiring institutions to take a more proactive approach.[150] Although the breach prevention regulations are more explicit in their requirements to preempt data breaches, the GLBA still asks that financial institutions implement their own security measures.[151] Implementing uniform state regulations would be consistent with the GLBA[152] and addresses one of the GLBA's initial critiques about being too prescriptive by allowing each entity to create its own method for compliance.[153] The breach prevention regulations also reinforce the Safeguards Rule's requirements about designating information security

[146] *Id.* § 6802(b) ("A financial institution may not disclose nonpublic personal information to a nonaffiliated third party unless . . . the consumer is given the opportunity, before the time that such information is initially disclosed, to direct that such information not be disclosed to such third party; and the consumer is given an explanation of how the consumer can exercise that nondisclosure option.").

[147] 16 C.F.R. § 314.1 (2017) (explaining the Federal Trade Commission will create a final Safeguards Rule, as required by section 501(b) of the Gramm-Leach-Bliley Act to establish standards relating to "administrative, technical and physical information safeguards" for financial institutions subject to the Commission's jurisdiction).

[148] *Id.* § 314.3(b).

[149] *See* N.Y. COMP. CODES R. & REGS. tit. 23, § 500.00 (2017) ("[T]his regulation is designed to promote the protection of customer information as well as the information technology systems of regulated entities.").

[150] Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice, 70 Fed. Reg. 15736, 15737 (proposed Aug. 7, 2001) (to be codified at 16 C.F.R. § 314) (providing an introduction to the GLBA and its focus on requiring every financial institution to implement a breach response system).

[151] *Id.* ("The introductory paragraph [of the GLBA] states that every financial institution should develop and implement security measures designed to address incidents of unauthorized access to customer information that occur despite measures to prevent security breaches.").

[152] *See id.* at 15739 ("[F]inancial institution should implement those security measures designed to prevent unauthorized access to or use of customer information, such as by placing access controls on customer information systems and conducting background checks for employees who are authorized to access customer information.").

[153] *Id.* ("[M]ost industry commenters thought that the proposed Guidance was too prescriptive. These commenters stated that the proposed approach would stifle innovation and retard the effective evolution of response programs.").

personnel and programs, identifying the potential risks, re-evaluating if new circumstances arise, and using third parties that will maintain the existing safeguards.[154] However, the NYDFS regulation adds two more technical safeguards, encryption and multi-factor authentication, that do not currently exist within the FTC regulation.[155]

Aside from the aforementioned statute and regulation, federal administrations have also pushed for more stringent cybersecurity protections.[156] In 2013, President Barack Obama issued an executive order calling for the improvement of "critical infrastructure cybersecurity" and the creation of "Cybersecurity Framework" by the National Institute of Standards and Technology.[157] The Framework was created with a focus on identifying, protecting, detecting, and responding to cybersecurity risks.[158] Included in the Framework are suggestions regarding risk management and an emphasis on evolving, organization-wide practices[159] as well as steps to creating an effective cybersecurity program.[160] The Framework, which was updated in 2017, not only incidentally provides guidance on NYDFS' breach prevention regulations, but further enforces a nationwide call to action on the issue of cybersecurity.[161]

[154] N.Y. COMP. CODES R. & REGS. tit. 23, § 500; *Financial Institutions and Customer Information: Complying with the Safeguards Rule*, FED TRADE COMM'N (Apr. 2006), https://www.ftc.gov/tips-advice/business-center/guidance/financial-institutions-customer-information-complying.

[155] Theodore P. Augustinos, *New York's Cybersecurity Requirements for DFS Licensees: A New Item at the Top of the To-Do List*, 29 INTELL. PROP. & TECH. L. J. 12, NO. 5 (2017).

[156] *See* Exec. Order No. 13636, 78 Fed. Reg. 11737 (Feb. 12, 2013) ("Repeated cyber intrusions into critical infrastructure demonstrate the need for improved cybersecurity. The cyber threat to critical infrastructure continues to grow and represents one of the most serious national security challenges we must confront.").

[157] *See* Improving Critical Infrastructure Cybersecurity, 78 Fed. Reg. 11737, 11741 (2013) ("The Cybersecurity Framework shall include a set of standards, methodologies, procedures, and processes that align policy, business, and technological approaches to address cyber risks.").

[158] NAT'L INSTITUTE OF STANDARDS & TECH., FRAMEWORK FOR IMPROVING CRITICAL INFRASTRUCTURE CYBERSECURITY 8 (2014).

[159] *See id.* at 11 ("Through a process of continuous improvement incorporating advanced cybersecurity technologies and practices, the organization actively adapts to a changing cybersecurity landscape and responds to evolving and sophisticated threats in a timely manner.").

[160] *Id.* at 13-15 (beginning with prioritizing business objectives and ending with implementation of an action plan).

[161] *Id.* at 2 ("The national and economic security of the United States depends on the reliable functioning of critical infrastructure. Cybersecurity threats exploit the increased

VI. CONCLUSION

The NYDFS regulations have the potential to be a successful model for other states, especially more so than simple data breach notification statutes.[162] The uniformity established in the early 2000s through such statutes demonstrates the nation's ability to stand behind one standard.[163] By creating uniform state regulations, each state will be able to use the New York regulations as a model while also using its own regulatory expertise to determine what methods for implementation are most realistic for that state.[164] As financial institutions continue to conduct business across states, establishing consistent regulations will eliminate confusion and the possibility for unintended liability.[165] The cybersecurity program, policy, incident response plan, and designated personnel combined are likely to help achieve the desired result of reducing data breaches.[166] However, as more regulations potentially develop, states should consider specifying the requirements of a cybersecurity program and providing more guidance to institutions on how these programs should be structured to adequately protect consumer data.

SABRINA GALLI[*]

complexity and connectivity of critical infrastructure systems, placing the Nation's security, economy, and public safety and health at risk.").

[162] *See supra* Part IV.

[163] NAT'L CONFERENCE OF STATE LEGISLATURES, *supra* note 32.

[164] *See supra* Part IV.

[165] *See supra* Part II (explaining the inadequacies of the breach notification statutes); *see also supra* Part IV (explaining the measures taken in creating the breach prevention statutes to remedy statutory inadequacies).

[166] *See supra* Part IV.

[*] I am particularly grateful to Professor Lissa Broome, Edward McCartney, Graham Dean, and the other editors for their thoughtful comments and guidance during the editing process. Further, I would like to thank my family for their constant support throughout my academic career.