HUNTON ANDREWS KURTH

Lawyer Insights

NEW YORK - CYBERSECURITY (NON-EU)

By Brittany Bacon, Michael La Marca and Lisa Xia
Published in OneTrust DataGuidance | June 2020

1. GOVERNING TEXTS

At their most general level, cybersecurity laws and standards are designed to protect against unauthorized access to and use, destruction, modification or disclosure of personal information. In contrast, privacy laws generally regulate the use, disclosure and other processing of personal information and may grant individuals with certain rights in connection with their personal information. While there is no comprehensive privacy law in the State of New York, in 2019, New York enacted a data security law that imposes security requirements that are generally applicable to businesses that own or license computerized data that includes the “private information” of New York residents. Prior to 2019, New York had in place sector-specific data security laws in the finance, health and education sectors. For example, the New York State Department of Financial Services adopted cybersecurity regulations establishing a robust set of cybersecurity requirements for New York financial services companies. In addition, the state has long required businesses to (1) provide notice to regulators and individuals in the event of certain data breaches; and (2) dispose of records containing personal identifying information in a secure manner.

Section 1 provides a high level overview of the general and sectoral legislation in New York, the regulators that are authorized to enforce these laws, and a brief summary of the guidance these regulators have issued. Sections 2 and 3 summarize the scope and requirements of the cybersecurity laws that regulate businesses generally in New York. Section 4 provides an overview of the sector-specific cybersecurity requirements in New York. Penalties for noncompliance with each of these laws are described in Section 5.

1.1. LEGISLATION

General Legislation

On July 25, 2019, New York Governor Andrew Cuomo signed into law the *Stop Hacks and Improve Electronic Data Security Act* (SHIELD Act), which amended the state’s general business law to require the implementation of reasonable security measures by businesses owning or licensing computerized data that includes the “private information” of New York residents. The amendment went into effect on March 21, 2020, and requires businesses to develop, implement and maintain reasonable safeguards to

This article presents the views of the authors, which do not necessarily reflect those of Hunton Andrews Kurth LLP or its clients. The information presented is for general information and education purposes. No legal advice is intended to be conveyed; readers should consult with legal counsel with respect to any legal advice they require related to the subject matter of the article. Receipt of this article does not constitute an attorney-client relationship. Prior results do not guarantee a similar outcome. Attorney advertising.

protect the security, confidentiality and integrity of private information.[1] The SHIELD Act specifies a non-exhaustive list of 14 administrative, technical and physical safeguards that businesses must implement to be deemed in compliance with the law. The law takes into account a business's size, complexity and activities, and does not impose additional requirements on entities subject to certain existing or future regulations by federal or New York State government entities.

In addition, the general business law that New York amended in 2019 already had required businesses to provide notice to regulators and individuals in the event of data breaches. New York expanded these breach notification requirements in 2019 in connection with its enactment of the SHIELD Act.

New York's general business law also prohibits businesses from disposing of records containing personal identifying information unless the entity takes certain actions to help ensure that no unauthorized person will have access to the information in the record.[2]

Sectoral Legislation

In 2017, the New York State Department of Financial Services (NYDFS) adopted regulations that established a robust set of cybersecurity requirements for New York financial services providers (Cybersecurity Regulation).[3] The Cybersecurity Regulation, which went into effect on March 1, 2017, requires covered entities to implement a comprehensive information security program that includes certain policies, procedures, guidelines and technical controls.

N.Y. Education Law § 2-d went into effect in April 2014 and provides protections for student data and for breaches of the responsibility to maintain the security and confidentiality of such data. N.Y. Education Law § 2-d requires the Commissioner of Education, in consultation with the chief privacy officer, to promulgate regulations establishing certain implementing procedures.[4] In January 2019, the New York State Education Department (NYSED) proposed implementing regulations that would require school districts and state-approved schools to develop and put in place robust data security and privacy policies. On January 13, 2020, the Board of Regents formally adopted a modified version of the proposed draft regulations. These regulations became effective on January 29, 2020.

1.2. SUPERVISORY AUTHORITIES

In New York, the Attorney General (AG) has enforcement authority over unfair and deceptive business practices under the state's consumer protection law. Although the SHIELD Act does not explicitly provide the AG with enforcement authority, the SHIELD Act deems violations of the law to be a deceptive

[1] N.Y. Gen. Bus. Law § 899-bb(2).

[2] N.Y. Gen. Bus. Law § 399-h.

[3] 23 NYCRR 500.

[4] N.Y. Educ. Law § 2-d(2) (McKinney).

business practice. The AG also has the power to bring actions to address improper disposal of records and violations of the state's breach notification requirements.[5]

Sector-specific regulators often are charged with enforcing the laws that regulate their respective industries. For example, the NYDFS, which was created in 2011, consolidated the New York State Banking Department and the New York State Insurance Department into one agency so that a single agency could "oversee a broader array of financial products and services." The superintendent of the NYDFS may enforce the Cybersecurity Regulation with respect to entities under its jurisdiction.

The NYSED is responsible for promoting data privacy and security information practices and policies at state educational agencies. Upon receipt of a complaint or other information indicating that an improper disclosure by a third-party contractor may have occurred, the chief privacy officer[6] is authorized to investigate, visit, examine and inspect the third-party contractor's facilities and records and obtain documentation from, or require the testimony of, any party relating to the alleged improper disclosure of student data, or teacher or principal data.[7]

1.3. REGULATORY AUTHORITY GUIDANCE

The NYDFS maintains a comprehensive list of FAQs about the Cybersecurity Regulation on its website.[8] The FAQs cover a wide range of topics including, for example, information about: (1) what constitutes a covered entity and the applicability of the law to out-of-state domestic banks or out-of-country foreign banks; (2) the level of due diligence and monitoring required; (3) when an unsuccessful attack has or had a "reasonable likelihood of materially harming any material part of the normal operation(s) of the [c]overed [e]ntity"; (4) when a covered entity is required to report a cybersecurity event under 23 NYCRR 500.17(a) and how to make such a report; (5) administrative aspects of the law, such as who may file or when to file a certificate of compliance and other notices; (6) how covered entities may address cybersecurity issues with respect to certain types of companies (e.g., a bank holding company); (7) how covered entities may address cybersecurity issues with respect to their subsidiaries and affiliates; (8) obligations of covered

[5] N.Y. Gen. Bus. Law § 899-aa(6); N.Y. Gen. Bus. Law § 399-h(3).

[6] The Commissioner of Education is required to appoint within the department a chief privacy officer with "training or experience in state and federal education privacy laws and regulations, civil liberties, information technology, and information security." N.Y. Educ. Law § 2-d(2) (McKinney). The Chief Privacy Officer's functions include promoting the implementation of sound information practices for the privacy and security of student data, or teacher or principal data, and assisting the Commissioner in handling data breaches and in due process proceedings regarding any alleged breaches of student data, or teacher or principal data. *Id.*

[7] *Id.* Specifically, the implementing regulations authorize the chief privacy officer to access "all records, reports, audits, review, documents, paper, recommendations, and other materials maintained by an educational agency that relate to student data or teacher or principal data," including records related to any technology product or service used to store or process personally identifiable information. Based on the records, the chief privacy officer is permitted to require an educational agency to ensure that all personally identifiable information is protected in accordance with state and federal laws and regulations, including by requiring an educational agency to perform a privacy impact and security risk assessment. Part 121 of the Regulations of the Commissioner of Education, § 121.13.

[8] FAQs: 23 NYCRR Part 500 – Cybersecurity, N.Y. DEP'T FIN. SERVS., https://www.dfs.ny.gov/industry_guidance/cyber_faqs.

entities when acquiring or merging with a new company; (9) when covered entities may rely on the cybersecurity program of another covered entity; (10) exemptions, including a chart summarizing the requirements a covered entity still must comply with if a limited exemption applies; and (11) other general compliance information.

The NYSED also maintains on its website a list of FAQs about data privacy and security, such as questions and answers that: (1) describe steps to take in the event of a breach of confidentiality or security; (2) discuss the contractual provisions that must be included in educational agencies' contracts with third-party contractors; and (3) provide information on the kinds of student data that are and are not subject to the confidentiality and security requirements of N.Y. Education Law § 2-d.[9]

2. SCOPE OF APPLICATION

The SHIELD Act applies to any person or business owning or licensing computerized data that includes the private information of a New York resident.[10] "Private information" means either: (1) personal information (i.e., any information concerning a natural person which, because of name, number, personal mark or other identifier, can be used to identify such natural person) consisting of any information in combination with any one or more of the following data elements, when either the data element or the combination of personal information plus the data element is not encrypted, or is encrypted with an encryption key that has also been accessed or acquired: (a) Social Security number; (b) driver's license number or non-driver identification card number; (c) account number, credit card number or debit card number, in combination with any required security code, access code, password or other information that would permit access to an individual's financial account; (d) account number, credit card number or debit card number, if circumstances exist wherein such number could be used to access an individual's financial account without additional identifying information, security code, access code or password; or (e) biometric information; or (2) a user name or email address in combination with a password or security question and answer that would permit access to an online account. The term does not include publicly available information that is lawfully made available to the general public from federal, state or local government records.[11]

Notably, although the SHIELD Act applies to all businesses, the law provides certain flexibility to "small businesses," which are permitted to consider their size, complexity and business activities in determining the reasonable safeguards to implement.[12] As defined by the SHIELD Act, a "small business" includes any person or business with: (1) fewer than 50 employees; (2) less than $3 million in gross annual revenue in each of the last three fiscal years; or (3) less than $5 million in year-end total assets.[13]

[9] Frequently Asked Questions About Data Privacy and Security, N.Y. EDU. DEP'T, http://www.nysed.gov/data-privacy-security/frequently-asked-questions-about-data-privacy-and-security.

[10] N.Y. Gen. Bus. Law § 899-bb(2).

[11] N.Y. Gen. Bus. Law § 899-bb(1)(b).

[12] N.Y. Gen. Bus. Law § 899-bb(2)(c).

[13] N.Y. Gen. Bus. Law § 899-bb(1)(c).

The state's breach notification law, which was expanded by the SHIELD Act, also applies to any person or business owning or licensing computerized data that includes the private information of a New York resident. In addition, the state's records disposal law applies to any person, business, firm, partnership, association or corporation that disposes of records containing personal identifying information. Under this law, "personal identifying information" means personal information consisting of any information in combination with any one or more of the following data elements (when either the personal information or the data element is not encrypted, or encrypted with an encryption key that is included in the same record as the encrypted personal information or data element): (1) Social Security number; (2) driver's license number or non-driver identification card number; or (3) mother's maiden name, financial services account number or code, savings account number or code, checking account number or code, debit card number or code, automated teller machine number or code, electronic serial number or personal identification number (i.e., any number or code which may be used alone or in conjunction with any other information to assume the identity of another person or access financial resources or credit of another person).[14]

3. REQUIREMENTS

3.1. SECURITY MEASURES

The SHIELD Act requires businesses to develop, implement and maintain reasonable safeguards to protect the security, confidentiality and integrity of private information.[15] A business will be deemed to be in compliance with the SHIELD Act's reasonableness standard if it implements a data security program that includes:

- ***Reasonable administrative safeguards***, such as: (1) designating one or more employees to coordinate the security program; (2) identifying reasonably foreseeable internal and external risks; (3) assessing the sufficiency of safeguards in place to control the identified risks; (4) training and managing employees in the security program practices and procedures; (5) selecting service providers capable of maintaining appropriate safeguards and requiring those safeguards by contract; and (6) adjusting the security program in light of business changes or new circumstances.[16]

- ***Reasonable technical safeguards***, such as: (1) assessing risks in network and software design; (2) assessing risks in information processing, transmission and storage; (3) detecting, preventing and responding to attacks or system failures; and (4) regularly testing and monitoring the effectiveness of key controls, systems and procedures.[17]

[14] N.Y. Gen. Bus. Law § 399-h.

[15] N.Y. Gen. Bus. Law § 899-bb(2).

[16] N.Y. Gen. Bus. Law § 899-bb(2)(b)(ii)(A)(1)–(6).

[17] N.Y. Gen. Bus. Law § 899-bb(2)(b)(ii)(B)(1)–(4).

- ***Reasonable physical safeguards***, such as: (1) assessing risks of information storage and disposal; (2) detecting, preventing and responding to intrusions; (3) protecting against unauthorized access to or use of private information during or after the collection, transportation and destruction or disposal of the information; and (4) disposing of private information within a reasonable amount of time after it is no longer needed for business purposes by erasing electronic media so that the information cannot be read or reconstructed.[18]

As described in Section 2 above, the law provides a more flexible standard for small businesses. Under the law, a small business is considered to be compliant if it has implemented reasonable administrative, technical and physical safeguards appropriate for the size and complexity of the small business, the nature and scope of the small business's activities, and the sensitivity of the personal information the small business collects from or about consumers.[19]

The SHIELD Act also provides that a business will be deemed to be in compliance with the law if the business is subject to and in compliance with: (1) regulations promulgated pursuant to Title V of the federal Gramm-Leach-Bliley Act (GLBA); (2) regulations implementing the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the Health Information Technology for Economic and Clinical Health Act (HITECH Act); (3) the NYDFS Cybersecurity Regulation; or (4) any other data security rules and regulations of, and the statutes administered by, any official department, division, commission or agency of the federal or New York state government as such rules, regulations or statutes are interpreted by such department, division, commission or agency or by the federal or New York state courts (collectively, "Other Federal and New York State Rules").[20]

3.2. NOTIFICATION OF CYBERSECURITY INCIDENTS

New York's general business code contains the state's data breach notification law, which requires any person or business owning or licensing computerized data that includes private information to disclose any "breach of the security of the system" to any New York resident whose private information was (or is reasonably believed to have been) accessed or acquired by a person without valid authorization. [21] If notice to affected individuals is required, the law also obligates the business to notify the following government agencies: (1) the state AG; (2) the Department of State Division of Consumer Protection; and (3) the Division of State Police.[22] Any person or business that maintains computerized data that includes private information that such person or business does not own (e.g., a vendor that processes private information on a business's behalf) must notify the owner or licensee of the information of any breach of

[18] N.Y. Gen. Bus. Law § 899-bb(2)(b)(ii)(C)(1)–(4).

[19] N.Y. Gen. Bus. Law § 899-bb(2)(c).

[20] N.Y. Gen. Bus. Law § 899-bb(2)(b)(i).

[21] N.Y. Gen. Bus. Law § 899-aa(2).

[22] N.Y. Gen. Bus. Law § 899-aa(2)(b).

the security of the system if the private information was (or is reasonably believed to have been) accessed or acquired by a person without valid authorization.[23]

Pursuant to the law, a “breach of the security of the system” means unauthorized access to or acquisition of (or access to or acquisition without valid authorization) computerized data that compromises the security, confidentiality or integrity of private information maintained by a business.[24] In determining whether information has been *accessed* (or is reasonably believed to have been accessed) by an unauthorized person or a person without valid authorization, the breach notification law specifies that the business may consider, among other factors, indications that the information was viewed, communicated with, used or altered by a person without valid authorization or by an unauthorized person.[25] In determining whether information has been *acquired* (or is reasonably believed to have been acquired) by an unauthorized person or a person without valid authorization, the business may consider, among other factors, indications that (1) the information is in the physical possession and control of an unauthorized person, such as a lost or stolen computer or other device containing the information; (2) the information has been downloaded or copied; or (3) the information was used by an unauthorized person (e.g., fraudulent accounts opened or instances of identity theft reported).[26]

The law provides that good faith access to or acquisition of private information by an employee or agent of the business entity for the purposes of the business would not be considered a notifiable breach, provided that the private information is not used or subject to unauthorized disclosure.[27]

Individual Notification

As described above, any person or entity that owns or licenses computerized data that includes private information is required to notify New York residents affected by a breach of the security of the system (i.e., those whose private information was, or is reasonably believed to have been, accessed or acquired by a person without valid authorization).[28]

The affected New York residents must be notified without unreasonable delay, consistent with the legitimate needs of law enforcement or any measures necessary to determine the scope of the breach and restore the integrity of the system.[29] Notification must include: (1) contact information for the person or business making the notification; (2) the telephone numbers and websites of the relevant state and federal agencies that provide information regarding security breach response and identity theft prevention and protection; and (3) a description of the categories of information that were (or are reasonably

[23] N.Y. Gen. Bus. Law § 899-aa(3).

[24] N.Y. Gen. Bus. Law § 899-aa(1)(c).

[25] *Id.*

[26] *Id.*

[27] *Id.*

[28] N.Y. Gen. Bus. Law § 899-aa(2).

[29] *Id.*

believed to have been) accessed or acquired without valid authorization, including a specification of which elements of personal information and private information were, or are reasonably believed to have been, accessed or acquired.[30]

The entity that experienced the breach must provide written or telephonic notice, or electronic notice if the person has expressly consented to such notice in electronic form.[31] Substitute notification also is acceptable if the business demonstrates that: (1) the cost of providing notice would exceed $250,000; (2) the affected class of subject persons to be notified exceeds 500,000; or (3) the business does not have sufficient contact information to provide notice through one of the methods described above.[32] Substitute notification consists of *all* of the following: (1) email notice (if the business has an email address for the affected New York residents), unless the breached information includes an email address in combination with passwords or security questions and answers that would permit access to the online account, in which case the person or business instead must provide clear and conspicuous notice delivered to the affected individuals online when the affected individual is connected to the online account from an Internet Protocol address, or from an online location which the person or business knows the consumer customarily uses to access the online account; (2) conspicuous posting of the notice on the business's website, if the business maintains a website; and (3) notification to state-wide media.[33]

New York's breach notification law provides certain exemptions to the obligation to notify affected individuals in the event of a breach of the security of the system. Specifically, affected individuals are not required to be notified if (1) the exposure of private information was an inadvertent disclosure by persons authorized to access private information, and (2) the person or business reasonably determines that such exposure will not likely result in misuse of such information, financial harm to the affected persons or, in the case of certain unknown disclosures of online credentials, emotional harm. In these instances where a business determines that notice is not required, the business must document its determination in writing and maintain the documentation for at least five years.[34] Further, if the private information of over 500 individuals is exposed, the business must provide the written determination to the state AG within ten days after the determination.[35]

In addition, a business is not required to notify affected individuals of a breach of the security of the system if the business otherwise provides such notice pursuant to any of the following legal requirements:

[30] N.Y. Gen. Bus. Law § 899-aa(7).

[31] N.Y. Gen. Bus. Law § 899-aa(5)(a)–(c). Electronic notice to an individual is permitted, "provided that the person has expressly consented to receiving said notice in electronic form and a log of each such notification is kept by the person or business who notifies affected persons in such form." N.Y. Gen. Bus. Law § 899-aa(5)(b). Businesses providing telephonic notification also must retain a log of each such notification. N.Y. Gen. Bus. Law § 899-aa(5)(c).

[32] N.Y. Gen. Bus. Law § 899-aa(5)(d).

[33] N.Y. Gen. Bus. Law § 899-aa(5)(d)(1)–(3).

[34] N.Y. Gen. Bus. Law § 899-aa(2)(a).

[35] *Id.*

(1) regulations promulgated pursuant to the GLBA; (2) HIPAA and the HITECH Act; (3) the NYDFS Cybersecurity Regulation; or (4) Other Federal and New York State Rules.[36]

Regulator Notification

In general, if New York residents must be notified, the business also must notify the state AG, the Department of State Division of Consumer Protection, and the Division of State Police. Notification to these regulatory bodies must be made without delaying notice to affected New York residents and include the timing, content and method of distribution of the notices to affected individuals, the approximate number of affected persons, and a copy of the template of the notice sent to affected individuals.[37]

Businesses must notify the New York regulators under the state's breach notification law even if the law does not require notice to affected individuals because such notice has been provided pursuant to: (1) the GLBA; (2) HIPAA and the HITECH Act; (3) the NYDFS Cybersecurity Regulation; or (4) Other Federal and New York State Rules.[38] In addition, if an entity is required to provide notification of a breach to the Secretary of Health and Human Services pursuant to HIPAA, including a breach of information that is not considered "private information" under New York's state breach notification law, the covered entity still is required under the law to provide notification to the state AG and must do so within five business days of notifying the Secretary of Health and Human Services.[39]

Notification to Consumer Reporting Agencies

If a business is required to notify more than 5,000 New York residents, the business also is required to notify consumer reporting agencies as to the timing, content and distribution of the notices, as well as the approximate number of affected individuals.[40] This notice must be made without delaying notice to affected New York residents.

Notably, businesses are required to notify consumer reporting agencies under the state's breach notification law even if the business notified affected individuals under: (1) the GLBA; (2) HIPAA and the HITECH Act; (3) the NYDFS Cybersecurity Regulation; or (4) Other Federal and New York State Rules.[41]

Vendor Notification

As described above, the state's breach notification law requires any person or business maintaining computerized data that includes private information that such person or business does not own to immediately notify the owner or the licensee of the information of any breach of the security of the system

[36] N.Y. Gen. Bus. Law § 899-aa(2)(b).

[37] N.Y. Gen. Bus. Law § 899-aa(8)(a).

[38] N.Y. Gen. Bus. Law § 899-aa(2)(b).

[39] N.Y. Gen. Bus. Law § 899-aa(9).

[40] N.Y. Gen. Bus. Law § 899-aa(8)(b).

[41] N.Y. Gen. Bus. Law § 899-aa(2)(b).

if the private information was (or is reasonably believed to have been) accessed or acquired by a person without valid authorization.[42]

Notification Required of State Agencies

The New York State Technology Law contains similar breach notification requirements that apply to state agencies.[43] These notification requirements largely are similar to those required by the general state breach notification law, but instead apply to state agencies owning or licensing computerized data that includes private information.

At a high level, like businesses, agencies are required to disclose any "breach of the security of the system" to any New York resident whose private information was (or is reasonably believed to have been) accessed or acquired by a person without valid authorization.[44] If notice to affected individuals is required, the agency also must notify consumer reporting agencies and the following state regulators: (1) the state AG; (2) the Department of State Division of Consumer Protection; and (3) the Office of Information Technology Services.[45] Any agency maintaining computerized data that includes private information that such agency does not own (e.g., a vendor that processes private information on an agency's behalf) must notify the owner or licensee of the information of any breach of the security of the system if the private information was (or is reasonably believed to have been) accessed or acquired by a person without valid authorization.[46] The processes for notifying each of the relevant parties are similar to the processes required by the state breach notification described above with a few minor differences. These requirements are enforced by the Office of Information Technology Services. There are no penalties for non-compliance.

4. SECTOR-SPECIFIC REQUIREMENTS

Cybersecurity in the health sector

Although the SHIELD Act does not specifically apply to health information, entities in the health sector also must ensure compliance with the law's data security and breach notification requirements. As described above, the SHIELD Act requires any person or business owning or licensing computerized data that includes the private information of a New York resident—including HIPAA-covered entities that own or license computerized data that includes the private information of a New York resident—to "develop,

[42] N.Y. Gen. Bus. Law § 899-aa(3).

[43] N.Y. State Tech. Law § 208. Specifically, the law applies to "any state board, bureau, division, committee, commission, council, department, public authority, public benefit corporation, office or other governmental entity performing a governmental or proprietary function for the state of New York, except: (1) the judiciary; and (2) all cities, counties, municipalities, villages, towns and other local agencies." N.Y. State Tech. Law § 208(1)(c).

[44] N.Y. State Tech. Law § 208(2).

[45] N.Y. State Tech. Law § 208(2)(b). Recall that non-agency businesses also must notify the state AG and the Department of State Division of Consumer Protection. Instead of notifying the Office of Information Technology Services, however, businesses are required to notify the Division of State Police.

[46] N.Y. State Tech. Law § 208(3).

implement and maintain reasonable safeguards to protect the security, confidentiality and integrity of the private information."[47] Notwithstanding the above, the law provides that, if a HIPAA-covered entity is compliant with the HIPAA and HITECH Act data security requirements, the entity also will be deemed to be compliant with the SHIELD Act's data security requirement.

Moreover, even though a HIPAA-covered entity that provides notice of a breach to affected individuals pursuant to the HIPAA breach notification rule is not required to make an additional notification to affected New York residents under the state's breach notification law (as amended by the SHIELD Act), the entity still must notify the New York Attorney General, the Department of State, the Division of State Police and, if more than 5,000 New York residents must be notified, the consumer reporting agencies. Where a HIPAA-covered entity must notify the Secretary of Health and Human Services of a breach pursuant to HIPAA and the HITECH Act, the entity also must provide notice to the New York Attorney General's office within five business days of the notification to the Secretary of Health and Human Services, even if "private information" (as defined by the SHIELD Act) is not impacted.

In August 2019, after the SHIELD Act passed but before the SHIELD Act's breach notification provisions became effective, the New York State Department of Health (DOH) issued a letter requiring certain health care providers to inform their DOH Regional Office in the event of a potential cybersecurity incident.[48] A cybersecurity incident is defined in the notice as "the attempted or successful unauthorized access, use, disclosure, modification, or destruction of data or interference with an information system operations."[49] The letter stated that the protocol be implemented immediately by hospitals, nursing homes, diagnostic and treatment centers, adult care facilities, home health agencies, hospices and licensed home care services agencies. The notification to the DOH Regional Office is in addition to any other notifications required under state or federal regulation.

For more information on the SHIELD Act, please refer to Sections 1-3 above and Section 5 below.

Cybersecurity in the financial sector

As described in Section 1 above, in 2017, regulations were adopted by the NYDFS that established a robust set of cybersecurity requirements for New York financial services providers.[50] Applicable to all individuals and non-governmental entities operating under or required to operate under a license, registration, charter or other form of authorization pursuant to New York banking, insurance or financial services law,[51] the Cybersecurity Regulation went into effect on March 1, 2017, and requires such covered entities to maintain a comprehensive written cybersecurity program that meets certain prescribed

[47] N.Y. Gen. Bus. Law § 899-bb(2).

[48] New York Dep't of Health, Notice Letter, Notification 101799 (Aug. 12, 2019).

[49] *Id*.

[50] 23 NYCRR 500.

[51] 23 NYCRR 500.01(c).

criteria. As part of its cybersecurity program, a covered entity must implement various policies, procedures, guidelines and technical controls as provided by the Cybersecurity Regulation.

At a high level, the foundational requirement of the Cybersecurity Regulation is for each covered entity to maintain a cybersecurity program that is designed to protect the confidentiality, integrity and availability of the covered entity's “information systems” and “nonpublic information” stored on those information systems.[52] Under the Cybersecurity Regulation, “information systems” are defined broadly to contemplate most information technology resources and specialized systems such as industrial control systems, telephone switching systems and environmental control systems.[53] “Nonpublic information” is defined under the Cybersecurity Regulation as data in electronic form that consists of certain categories of material business-related information, sensitive personal information and health information, to the extent the information is not publicly available. Specifically, “nonpublic information” includes all electronic information that is “not publicly available information” and is:

1. Business-related information of a covered entity, the tampering with which, or unauthorized disclosure, access, or use of which, would cause a material adverse impact to the business, operations or security of the covered entity;

2. 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: (a) Social Security number; (b) driver's license number or non-driver identification card number; (c) account number, credit or debit card number; (d) any security code, access code, or password that would permit access to an individual's financial account; or (e) biometric records; or

3. Any information or data, except age or gender, in any form or medium created by or derived from a health care provider or an individual and that relates to (a) the past, present, or future physical, mental, or behavioral health or condition of any individual or a member of the individual's family; (b) the provision of health care to any individual; or (c) payment for the provision of health care to any individual.[54]

The Cybersecurity Regulation’s requirements thus extend beyond the protection of personal information and apply to the safeguarding of “information systems” generally and material business-related information.

The Cybersecurity Regulation requires each covered entity to conduct and document a periodic risk

[52] 23 NYCRR 500.02.

[53] 23 NYCRR 500.01(e). “Information Systems” means “a discrete set of electronic information resources organized for the collection, processing, maintenance, use, sharing, dissemination or disposition of electronic information, as well as any specialized system such as industrial/process controls systems, telephone switching and private branch exchange systems, and environmental control systems.” *Id.*

[54] 23 NYCRR 500.01(g).

assessment of the entity's information systems that is sufficient to inform the design of the cybersecurity program.[55] The risk assessment must be updated as reasonably necessary to address changes to the entity's information systems, nonpublic information or business operations, and be sufficiently adaptable to allow for revision of controls to respond to technological developments and evolving threats. [56] In addition, the risk assessment must be carried out in accordance with policies and procedures that include (1) criteria for evaluating and categorizing identified cybersecurity risks or threats; (2) criteria for assessing the confidentiality, integrity, security and availability of the covered entity’s information systems and nonpublic information, including the adequacy of existing controls in the context of identified risk; and (3) requirements describing how identified risks will be mitigated or accepted based on the risk assessment and how the cybersecurity program will address the risks.[57]

The Cybersecurity Regulations indicate that the covered entity’s cybersecurity program must be based on the results of its comprehensive risk assessment. [58] Further, at a high level, the cybersecurity program must be designed to: (1) identify and assess cybersecurity risks that may threaten the security or integrity of nonpublic information stored on the covered entity's systems; (2) use defensive infrastructure and the implementation of policies and procedures to protect the entity's systems and the nonpublic information stored therein from unauthorized access, use or other malicious acts; (3) detect and respond to cybersecurity events and mitigate any negative effects; (4) recover from cybersecurity events and restore normal operations and services; and (5) fulfill applicable regulatory reporting obligations.[59]

In addition to the more general requirements cited above, as part of its overall cybersecurity program, covered entities are required to implement written policies and procedures that specifically address the following topics, to the extent applicable: (1) information security; (2) data governance and classification; (3) asset inventory and device management; (4) access controls and identity management; (5) business continuity and disaster recovery planning and resources; (6) systems operations and availability concerns; (7) systems and network security; (8) systems and network monitoring; (9) systems and application development and quality assurance; (10) physical security and environmental controls; (11) customer data privacy; (12) vendor and third-party service provider management; (13) risk assessment; and (14) incident response.[60] Moreover, the Cybersecurity Regulations include data retention restrictions that require covered entities to have in place policies and procedures for the secure disposal of certain types of nonpublic information on a periodic basis when the information is no longer necessary for business operations or for other legitimate business purposes of the entity, subject to certain exceptions.[61]

[55] 23 NYCRR 500.09.

[56] 23 NYCRR 500.09.

[57] *Id*.

[58] 23 NYCRR 500.02(b).

[59] 23 NYCRR 500.02(b).

[60] 23 NYCRR 500.03(a).

[61] 23 NYCRR 500.13.

In addition to written policies and procedures, as part of a covered entity's cybersecurity program, the Cybersecurity Regulation requires covered entities to implement certain cybersecurity controls and practices. These processes and technical controls must adhere to the numerous requirements set forth in the Cybersecurity Regulation related to: (1) performing ongoing monitoring, annual penetration testing and bi-annual vulnerability assessments;[62] (2) maintaining sufficient audit trails for systems;[63] (3) limiting and reviewing user access privileges to certain information systems;[64] (4) using qualified personnel to implement the entity's cybersecurity program and providing sufficient cybersecurity updates and training to such cybersecurity personnel;[65] (5) using multi-factor or risk-based authentication methods to protect against unauthorized access to certain nonpublic information or information systems;[66] (6) monitoring the activity of authorized users to detect unauthorized access or use of, or tampering with, nonpublic information;[67] (7) providing regular, updated cybersecurity awareness training for all personnel;[68] and (8) implementing encryption to protect nonpublic information in transit over external networks and at rest.[69]

Covered entities also are required to maintain additional documentation pertaining to specific cybersecurity management processes and guidelines. For example, covered entities must implement, in accordance with the Cybersecurity Regulation, written policies and procedures for managing the security of third-party service providers.[70] A covered entity's cybersecurity program also must include written procedures, guidelines and standards for developing and procuring secure software applications.[71] In

[62] 23 NYCRR 500.05.

[63] 23 NYCRR 500.06.

[64] 23 NYCRR 500.07.

[65] 23 NYCRR 500.10.

[66] 23 NYCRR 500.12.

[67] 23 NYCRR 500.14(a).

[68] 23 NYCRR 500.14(b).

[69] 23 NYCRR 500.15.

[70] 23 NYCRR 500.011. Specifically, each covered entity must implement written policies and procedures that are designed to ensure the security of information systems and nonpublic information that are accessible to, or held by, third-party service providers and address, to the extent applicable: (1) the identification and risk assessment of third-party service providers; minimum cybersecurity practices required to be met by third-party service providers; (3) due diligence processes used to evaluate the adequacy of the third-party service provider's cybersecurity practices; and (4) periodic assessment of third-party service providers based on the risk they present and the continued adequacy of their cybersecurity practices. The policies and procedures also must include guidelines for due diligence and/or contractual protections relating to third-party service providers, including, to the extent applicable, guidelines addressing (1) the third-party service provider's policies and procedures governing access controls (including multi-factor authentication) and encryption; (2) notice to be provided to the covered entity in the event of a cybersecurity event directly impacting the covered entity's information systems or nonpublic information held by the third-party service provider; and (3) representations and warranties addressing the third-party service provider's cybersecurity policies and procedures that relate to the covered entity's information systems or nonpublic information.

[71] 23 NYCRR 500.08.

addition, covered entities must establish a written incident response plan for responding to and recovering from cybersecurity events.[72]

The Cybersecurity Regulations require entities to report cybersecurity events to NYDFS as promptly as possible, but in no event later than 72 hours, after a determination that a cybersecurity event has occurred where (1) notice is required to be provided to any government body, self-regulatory agency or any other supervisory body, or (2) the event has a reasonable likelihood of materially harming any material part of the normal operations of the entity.[73] A "cybersecurity event" is defined as any act or attempt, successful or unsuccessful, to gain unauthorized access to, disrupt or misuse an information system or information stored on such system.[74]

Each covered entity also must designate a Chief Information Security Officer (CISO), or similarly qualified individual responsible for overseeing and implementing the covered entity's cybersecurity program and enforcing its cybersecurity policies and procedures.[75] Senior officials and boards of directors are assigned cybersecurity oversight responsibilities. For example, the covered entity's cybersecurity policies and procedures must be approved by a senior officer or the board of directors (or an equivalent governing body),[76] and the covered entity's board of directors or equivalent governing body must receive from the CISO (or the equivalent designated cybersecurity individual) an annual written report detailing the entity's cybersecurity program and material cybersecurity risks.[77] In addition, in connection with these oversight responsibilities, a senior officer or the board of directors must submit to the NYDFS an annual written statement certifying the entity's compliance with the Cybersecurity Regulation.[78]

The Cybersecurity Regulation exempts many of the requirements discussed above with respect to covered entities that are limited in size or operation. An entity may be exempt from certain requirements of the Cybersecurity Regulation to the extent the entity falls under a specific size threshold concerning (1) the size of the entity's workforce, or (2) the entity's gross annual revenue earnings or year-end total asset holdings.[79] A covered entity also may be exempt from certain requirements of the Cybersecurity Regulation to the extent it does not operate, use, maintain or control information systems or access,

[72] 23 NYCRR 500.016.

[73] 23 NYCRR 500.17(a).

[74] 23 NYCRR 500.01(d).

[75] 23 NYCRR 500.04.

[76] 23 NYCRR 500.03(a).

[77] 23 NYCRR 500.04(b).

[78] 23 NYCRR 500.17(b). Each covered entity must maintain all records, schedules and data supporting this certification for a period of five years for examination by NYDFS and, to the extent the covered entity has identified areas, systems or processes that require material improvement, updating or redesign, the covered entity must document the identification and the remedial efforts planned and underway to address such areas, systems or processes.

[79] 23 NYCRR 500.19(a).

generate, receive or possess nonpublic information.[80] In addition, to the extent an entity is an agent, employee, representative or designee of another covered entity, the former may be covered under the cybersecurity program of the latter, and need not develop its own cybersecurity program.[81] Any covered entity that qualifies for one of these exemptions must file a written notice with the NYDFS.[82] As discussed in Section 1.3 above, more information about the exemptions and the requirements a covered entity must comply with in the event a limited exemption applies can be found in the FAQs posted to the NYDFS website.

Cybersecurity practices for employees

Although the SHIELD Act does not specifically apply to employee information, employers that own or license computerized data that includes the private information of New York residents must comply with the SHIELD Act. To comply, the employer must "develop, implement and maintain reasonable safeguards to protect the security, confidentiality and integrity of the private information," including by providing notification of data breaches pursuant to the law's requirements.[83] For more information on the SHIELD Act, please refer to Sections 1-3 above and Section 5 below.

Cybersecurity in the educational sector

N.Y. Education Law § 2-d, which went into effect April 2014, provides protections for student data,[84] and teacher and principal data[85] for breaches of the responsibility to maintain the security and confidentiality of such data. Among other requirements, the law requires educational agencies in New York to develop a Parent's Bill of Rights for Data Privacy and Security (Parent's Bill of Rights) that "state[s] in clear and plain English terms that":

- A student's personally identifiable information[86] cannot be sold or released for any commercial purposes.
- Parents have the right to inspect and review the complete contents of their child's education record;

[80] 23 NYCRR 500.19(c).

[81] 23 NYCRR 500.19(b).

[82] 23 NYCRR 500.19(d).

[83] N.Y. Gen. Bus. Law § 899-bb(2).

[84] "Student data" means personally identifiable information from the student records of an educational agency. N.Y. Educ. Law § 2-d(1)(i) (McKinney).

[85] "Teacher or principal data" means personally identifiable information from student records of an educational agency.

[86] For purposes of this section, "personally identifiable information" as applied to student data means personally identifiable information as defined in section 99.3 of Title 34 of the Code of Federal Regulations implementing the Family Educational Rights and Privacy Act, 20 U.S.C. 1232g. As applied to teacher or principal data, the term means "personally identifiable information" as used in N.Y. Educ. Law § 3012-c (i.e., annual professional performance review data). N.Y. Educ. Law § 2-d(1)(j) (McKinney).

- State and federal laws protect the confidentiality of personally identifiable information, and safeguards associated with industry standards and best practices (e.g., encryption, firewalls and password protection) must be in place when data is stored or transferred;
- A complete list of all student data elements collected by the State is available for public review online or by mail (including the web address where it is available and the postal address from which it can be requested); and
- Parents have the right to have complaints about possible breaches of student data addressed and the phone number, email address and mailing address to which the complaints should be directed.[87]

The Parent's Bill of Rights also must include certain enumerated supplemental information about each contract an educational agency enters into with a third-party contractor, where the third-party contractor receives student data, or teacher or principal data.[88] Each educational agency's Parent's Bill of Rights must be posted on its website and be included with every contract the educational agency enters into with a third-party contractor, where the third-party contractor receives student data, or teacher or principal data.[89]

Education Law § 2-d also authorizes the Commissioner of Education to promulgate implementing regulations establishing standards for educational agencies' data security and privacy policies. In January 2019, the NYSED proposed regulations to require school districts and state-supported schools to develop and implement robust data security and privacy programs to protect any personally identifiable information relating to students, teachers and principals. On January 13, 2020, the Board of Regents formally adopted the regulations (with modifications).[90]

The regulations, which went into effect on January 29, 2020, require each state educational agency to adopt and publish by July 1, 2020, a data security and privacy policy that implements the requirements of regulations and that aligns with the National Institute for Standards and Technology Framework for Improving Critical Infrastructure Cybersecurity Version 1.1. (NIST Cybersecurity Framework).[91] The data

[87] N.Y. Educ. Law § 2-d (McKinney).

[88] Such supplemental information must include: (1) the exclusive purposes for which the student data or teacher or principal data will be used; (2) how the third-party contractor will ensure that the subcontractors, persons or entities that the third-party contractor will share the student data or teacher or principal data with, if any, will abide by data protection and security requirements; (3) when the agreement expires and what happens to the student data or teacher or principal data upon expiration of the agreement; (4) if and how a parent, student, eligible student, teacher or principal may challenge the accuracy of the student data or teacher or principal data that is collected; (5) where the student data or teacher or principal data will be stored (described in such a manner as to protect data security); and (6) the security protections taken to ensure such data will be protected, including whether such data will be encrypted. *Id.*

[89] *Id.*

[90] Strengthening Data Privacy and Security in NY State Educational Agencies to Protect Personally Identifiable Information, N.Y. STATE EDU. DEP'T, http://www.nysed.gov/data-privacy-security/regulations-strengthen-data-privacy-and-security.

[91] Part 121 of the Regulations of the Commissioner of Education, § 121.5.

security and privacy policy must be published on the educational agency's website and must include all protections afforded to parents or eligible students, where applicable, under FERPA and the Individuals with Disabilities Education Act, 20 U.S.C. 1400 *et seq.*, and implementing regulations.[92] Educational agencies are required to provide notice of the data security and privacy policy to all of their officers and employees.[93] Educational agencies also must provide to officers and employees with access to personally identifiable information annual data privacy and security awareness training that includes training on the state and federal laws that protect personally identifiable information, and how employees can comply with those laws.[94]

In addition, each educational agency that enters into a contract[95] with a third-party contractor must ensure that the contract includes the third-party contractor's data security and privacy plan that is accepted by the educational agency.[96] At a minimum, this data security and privacy plan must: (1) outline how the third-party contractor will implement all state, federal, and local data security and privacy contract requirements over the life of the contract, consistent with the educational agency's data security and privacy policy; (2) specify the administrative, operational and technical safeguards and practices it has in place to protect personally identifiable information that it will receive under the contract; (3) demonstrate that it complies with the requirements related to the Parent's Bill of Rights; (4) specify how officers or employees of the third-party contractor and its assignees who have access to student data, or teacher or principal data receive or will receive training on the federal and state laws governing confidentiality of such data prior to receiving access; (5) specify if the third-party contractor will utilize sub-contractors and how it will manage those relationships and contracts to ensure personally identifiable information is protected; (6) specify how the third-party contractor will manage data security and privacy incidents that implicate personally identifiable information, including specifying any plans to identify breaches and unauthorized disclosures, and to promptly notify the educational agency; and (7) describe whether, how and when data will be returned to the educational agency, transitioned to a successor contractor [or], at the educational agency's option and direction, deleted or destroyed by the third-party contractor when the contract is terminated or expires.[97]

Each third party contractor that receive student data or teacher or principal data is required under the regulations to: (1) adopt technologies, safeguards and practices that align with the NIST Cybersecurity

[92] Part 121 of the Regulations of the Commissioner of Education, § 121.5(d).

[93] Part 121 of the Regulations of the Commissioner of Education, § 121.5(e).

[94] Part 121 of the Regulations of the Commissioner of Education, § 121.7.

[95] Under the regulations, "contract or other written agreement" means a binding agreement between an educational agency and a third party, which shall include but not be limited to an agreement created in electronic form and signed with an electronic or digital signature or a click wrap agreement that is used with software licenses, downloaded and/or online applications and transactions for educational technologies and other technologies in which a user must agree to terms and conditions prior to using the product or service. Part 121 of the Regulations of the Commissioner of Education, § 121.1.

[96] Part 121 of the Regulations of the Commissioner of Education, § 121.6.

[97] *Id.*

Framework; (2) comply with the educational agency's data security and privacy policy, N.Y. Education Law § 2-d and the regulations; (3) limit internal access to personally identifiable information to only those employees or sub-contractors that need access to provide the contracted services; (4) not use the personally identifiable information for any purpose not explicitly authorized in its contract; (5) not disclose any personally identifiable information to any other party without the prior written consent of the parent or eligible student (except to certain authorized representatives of the third party contractor or unless required by law or court order and notice of disclosure is provided where applicable); (6) maintain reasonable administrative, technical and physical safeguards to protect the security, confidentiality and integrity of personally identifiable information in its custody; (7) use encryption to protect personally identifiable information in its custody while in motion or at rest; and (8) not sell personally identifiable information or use or disclose it for any marketing or commercial purpose or facilitate its use or disclosure by any other party for any marketing or commercial purpose or permit another party to do so.[98]

In addition, if a third-party contractor experiences any breach or unauthorized release of personally identifiable information, within seven days of discovery of the breach, it must notify each educational agency with which it has a contract.[99] Third-party contractors are required to cooperate with educational agencies and law enforcement in the event of an investigation into the breach or unauthorized release.[100] If a breach or unauthorized release is "attributed to" a third-party contractor, the third-party contractor must pay for or promptly reimburse the educational agency for the full cost of the notification.[101]

Educational agencies must report every discovery or report of a breach or unauthorized release of student, teacher or principal data to the chief privacy officer within 10 days of its discovery. Educational agencies also are required to notify affected parents, eligible students (i.e., students 18 years of age or older), teachers and principals within 60 calendar days after (1) discovery of the breach or unauthorized release by the educational agency, or (2) receipt of a notification of a breach or unauthorized release from a third-party contractor.[102] Notification may be delayed if such notification would interfere with an ongoing law enforcement investigation or cause further disclosure of personally identifiable information by disclosing an unfixed security vulnerability. If notification is delayed for these reasons, however, the educational agency must notify parents, eligible students, teachers and principals within seven calendar days after the risk of interference with law enforcement investigation ends or the security vulnerability has been remedied.[103]

The notification must be provided directly to the affected parent, eligible student, teacher or principal by first-class mail to their last known address, email or telephone, and must be clear, concise and easy to

[98] Part 121 of the Regulations of the Commissioner of Education, § 121.9.

[99] Part 121 of the Regulations of the Commissioner of Education, § 121.10(a).

[100] Part 121 of the Regulations of the Commissioner of Education, § 121.10(c).

[101] Part 121 of the Regulations of the Commissioner of Education, § 121.10(f).

[102] Part 121 of the Regulations of the Commissioner of Education, § 121.10(e).

[103] *Id.*

understand.[104] To the extent available, the notification should include: (1) a brief description of the breach or unauthorized release; (2) the dates of the incident and the date of discovery, if known; (3) a description of the types of personally identifiable information affected; (4) an estimate of the number of records affected; (5) a brief description of the educational agency's investigation or plan to investigate; and (6) contact information for representatives who can assist parents or eligible students that have additional questions.[105]

Each educational agency shall designate a data protection officer to be responsible for the implementation of the required policies and procedures. The individual designated for this role may be a current employee of the educational agency who performs this function in addition to other job responsibilities, but must have the appropriate knowledge, training and experience to effectively serve in this role.[106]

Each educational agency shall designate a data protection officer to be responsible for the implementation of the required policies and procedures. The individual designated this role may be a current employee of the educational agency who performs this function in addition to other job responsibilities, but must have the appropriate knowledge, training and experience to effectively serve in this role.[106]

Third-party contractors may be subject to penalties for non-compliance and may be subject to investigation by the chief privacy officer in connection with reports of breaches or unauthorized releases of student data, or teacher or principal data.[107] In addition, if the chief privacy officer determines that the third-party contractor has, through its actions or omissions, caused the data to be breached or released to an unauthorized person or entity, the chief privacy officer may impose strict orders on the third-party contractor that preclude the third-party contractor from accessing student data, or teacher or principal data for a set period of time.[108] If the breach or unauthorized release of data was inadvertent and done without intent, knowledge, recklessness or gross negligence, the chief privacy officer may make a recommendation of "no penalty."[109]

5. PENALTIES

At the state level, state AGs typically are charged with the authority to enforce privacy and data security obligations. In some instances, privacy and data security obligations are considered to be unlawful or

[104] Part 121 of the Regulations of the Commissioner of Education, § 121.10(g), (h).

[105] Part 121 of the Regulations of the Commissioner of Education, § 121.10(g).

[106] Part 121 of the Regulations of the Commissioner of Education, § 121.8.

[107] Part 121 of the Regulations of the Commissioner of Education, § 121.11.

[108] Part 121 of the Regulations of the Commissioner of Education, § 121.11(e).

[109] Part 121 of the Regulations of the Commissioner of Education, § 121.11(f).

deceptive business practices that are regulated by the state consumer protection law, which state AGs also enforce.

In New York, violations of the SHIELD Act are considered deceptive business practices, and the New York AG may bring an action to enjoin violations and obtain civil penalties of up to $5,000 per violation.[110] The New York AG also may bring an action to enjoin violations of the state's breach notification law.[111] In addition, businesses that violate the breach notification law may be subject to actual damages, including consequential damages, incurred by a person entitled to notice.[112] If the court determines that a business violated the breach notification law knowingly or recklessly, the business may be subject to a civil penalty of $5,000 or up to $20 per instance of failed notification (up to $250,000), whichever is greater.[113] Businesses that violate the state records disposal law may be subject to an injunction (even if there is no proof that any person has, in fact, been injured or damaged) and be subject to a civil penalty of up to $5,000 per violation.[114]

The NYDFS Cybersecurity Regulation does not include an express penalty. Rather, the Cybersecurity Regulation states only that the "regulation will be enforced by the superintendent pursuant to, and is not intended to limit, the superintendent's authority under any applicable laws."[115]

In the educational context, third-party contractors that receive student data, or teacher or principal data from an educational agency pursuant to a contract or other written agreement for services may be subject to civil penalties under N.Y. Education Law § 2-d and its implementing regulations. Under Education Law § 2-d, if a third-party contractor (or its assignee) fails to provide the required notification of a breach of security that results in an unauthorized release of student data, or teacher or principal data by the third-party contractor, the third-party contractor may be subject to a civil penalty of $5,000 or up to $10 per student, teacher and principal whose data was released (up to $250,000), whichever is greater.[116]

If any other provision of N.Y. Education Law § 2-d is violated by a third-party contractor (or its assignee), the third-party contractor may be subject to a civil penalty of up to $1,000. If the third-party contractor violates the same student data, or teacher or principal data a second time, the third-party contractor may be subject to a civil penalty of up to $5,000. Any additional violation of the same student data, or teacher

[110] N.Y. Gen. Bus. Law § 899-bb(d).

[111] N.Y. Gen. Bus. Law § 899-aa(6)(a). The state Attorney General has three years to commence an action from the date the Attorney General becomes aware of the violation or notice is sent to the Attorney General, whichever comes first. An action may not be brought after six years from the date of discovery of the breach of private information by the company unless the company took steps to hide the breach.

[112] *Id.*

[113] *Id.*

[114] N.Y. Gen. Bus. Law § 399-h. Acts arising out of the same incident or occurrence are considered to be a single violation. That a business used due diligence to properly dispose of records may be used as an affirmative defense. *Id.*

[115] 23 NYCRR 500.20.

[116] N.Y. Educ. Law § 2-d(6)(d) (McKinney).

or principal data is punishable by a civil penalty of up to $10,000. For purposes of the calculation of civil penalties, each violation is considered a separate violation. The total penalty, however, may not exceed $250,000.[117]

Brittany M. Bacon *is a partner in the firm's Global Privacy and Cybersecurity group in the firm's New York office. Brittany advises clients in identifying, evaluating and managing complex global privacy and information security risks and compliance issues. She can be reached at +1 (212) 309-1361 or bbacon@HuntonAK.com.*

Michael La Marca *is an associate in the firm's Global Privacy and Cybersecurity group in the firm's New York office. Mike advises multinational clients on compliance with all federal, state and international privacy and data security laws, and managing privacy and cybersecurity risks and policy issues. He can be reached at +1 (212) 309-1116 or mlamarca@HuntonAK.com.*

Lisa Xia *is an associate in the firm's Global Privacy and Cybersecurity group in the firm's New York office. She assists clients with the identification and management of legal risks associated with federal, state and international privacy and cybersecurity laws, and has worked with clients on compliance with the California Consumer Privacy Act of 2018. She can be reached at +1 (212) 309-1347 or lxia@HuntonAK.com.*

[117] N.Y. Educ. Law § 2-d(7)(b) (McKinney).