Katten

New York Stop Hacks and Improve Electronic Data Security Act

("SHIELD Act")

Effective March 21, 2020, "[a]ny person or business that owns or licenses computerized data which includes private information of a resident of New York shall develop, implement and maintain reasonable safeguards to protect the security, confidentiality and integrity of the private information." See below for exceptions for "*Small Businesses*" and "*Compliant Regulated Entities*."

Administrative safeguards

- ☐ *"Designate one or more employees to coordinate the security program."* Name specific personnel to implement and oversee the business's security program, presumably with appropriate knowledge and skill (e.g. a Chief Information Security Officer or someone with similar knowledge and skills) and appropriate authority and reporting lines to business leadership. The designated person is responsible for reporting any breaches to the New York State Attorney General's office and other applicable regulatory agencies.
- ☐ *"Identify reasonably foreseeable internal and external risks."* Perform initial and periodic risk assessments to identify risks and vulnerabilities to personal data and other sensitive and private information the business holds or processes, and determine and prioritize appropriate risk-based remediation or mitigation of identified risks.
- ☐ *"Assess the sufficiency of safeguards in place to control the identified risks."* Depending on the nature of the systems and data, include appropriate processes and protections, in terms of administrative controls – such as appropriate password policies – and technical controls as discussed below. Consider the extent to which employees need access to private information to perform their job responsibilities and limit privileges appropriately.
- ☐ *"Train and manage employees in the security program practices and procedures."* Provide new employees with security training during the onboarding process, and periodically train and test (e.g. phishing tests) existing employees.
- ☐ *"Select service providers capable of maintaining appropriate safeguards, and require those safeguards by contract."* Perform due diligence on – and consider periodic audits of – third party vendors who do or may have access to personal or sensitive information, to verify they maintain appropriate security controls. Include appropriate information security standards and requirements – and the ability to verify (e.g. right to audit and/or provision of third-party certifications such as SOC 2, ISO27001, PCI-DSS, etc.) – in all contracts to ensure service providers are required to maintain the applicable security standards.

Doron S. Goldstein
Partner
Privacy, Data and Cybersecurity
New York Office
+1.212.940.8840
doron.goldstein@katten.com

Megan Hardiman
Partner
Health Care
Chicago Office
+1.312.902.5488
megan.hardiman@katten.com

Trisha Sircar
Partner
Privacy, Data and Cybersecurity
New York Office
+1.212.940.8532
trisha.sircar@katten.com

- ☐ *"Adjust the security program in light of business changes or new circumstances."* At minimum, security programs should be reviewed on an annual basis to address changes to the business's operations and systems, information governance practices, and other relevant developments such as industry standards and practices.

Technical safeguards

- ☐ *"Assess risks in network and software design."* Consider the types of security threats a particular network or software system is susceptible to (e.g. brute force attacks, phishing attacks, denial of service (DDoS), identity spoofing, etc.) and implement appropriate technology to address those risks.
- ☐ *"Assess risks in information processing, transmission and storage."* Consider the risks to the data, and implement the technical processes to protect the date, including, as applicable, such as access management solutions, encryption standards, and multi-factor authentication.
- ☐ *"Detect, prevent and respond to attacks or system failures."* Implement systems and controls designed to prevent and detect attacks – such as firewalls, intrusion detection systems, logging and log monitoring, anti-malware systems, and email security systems – and prepare to respond to incidents by having and testing an appropriate incident response plan.
- ☐ *"Regularly test and monitor the effectiveness of key controls, systems and procedures."* Conduct periodic verification of systems and processing security, such as security audits, penetration testing, and tabletop/wargame exercises. Be sure to update and install patches to software and systems.

Physical safeguards

- ☐ *"Assess risks of information storage and disposal."* Consider whether the data (both electronic and physical copies) are held in appropriate locations, and how the data can be appropriately destroyed.
- ☐ *"Detect, prevent and respond to intrusions."* Implement appropriate monitoring of locations where data is held, such as monitored cameras and other systems, and ensure appropriate processes to respond to detected incidents.
- ☐ *"Protect against unauthorized access to or use of private information during or after the collection, transportation and destruction or disposal of the information."* Use safeguards to protect the physical locations where data are stored, such as, where appropriate, locked doors/cabinets, keycard access, clean desk procedures, and security guards.
- ☐ *"Dispose 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."* Implement appropriate record retention policies, and procedures for deleting or destroying electronic data when no longer necessary, such as NIST or other security standards for deletion and destruction procedures and safeguards.

Jeremy Merkel
Associate
Intellectual Property
New York Office
+1.212.940.6339
jeremy.merkel@katten.com

Dagatha L. Delgado
Staff Attorney
Intellectual Property
New York Office
+1.212.940.6350
dagatha.delgado@katten.com

Limited Exceptions

- ☐ **Small Businesses:** The SHIELD Act's requirement to implement a formal data security program does not apply to "small businesses," which is a business that has (i) fewer than fifty (50) employees; (ii) less than $3 million in gross annual revenue in each of the last three fiscal years; or (iii) less than $5 million in year-end total assets. Small businesses must still implement a security program that contains reasonable administrative, technical and physical safeguards that are 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.
- ☐ **Covered Regulated Entities**: Businesses that are regulated under, and comply with, the Gramm-Leach-Bliley Act (GLBA), the Health Insurance Portability and Accounting Act (HIPAA), the New York Department of Financial Services Cybersecurity Regulations, or other New York state data security rules and regulations are deemed in compliance with these requirements, to the extent that they comply with their applicable regulatory security requirements.