SHIELD and Sword:
New York's Far Reaching Statute Governing Data Breaches

Law.com – New York Law Journal
By David Jacoby and Linda V. Priebe

It may be a while before law enforcement can devote attention to the broadened scope of data breach liability under the new NY SHIELD (Stop Hacks and Improve Electronic Data Security) Act. Then again, it might not.

Important changes in New York's data privacy law took effect on March 21. But that was just two days after Gov. Andrew Cuomo declared the COVID-19 state of emergency, so you may not have been focusing closely on privacy law. If you didn't notice, however, rest assured you're not alone.

And it still may be a while before law enforcement can devote attention to the broadened scope of data breach liability under the new NY SHIELD (Stop Hacks and Improve Electronic Data Security) Act. Then again, it might not. Data protection regulators around the globe already are warning of increased risks to the security and privacy of personal information resulting from COVID-19 and increased remote work online, including fraud schemes and illicit sharing of health information. Even in the United States, the California Attorney General has announced that enforcement of that state's new Consumer Privacy Act (CCPA) will proceed on schedule beginning July 1, 2020 despite COVID-19. Fortunately, compliance with the NY SHIELD Act complements the CCPA and even the EU General Data Protection Regulation (GDPR) and so benefits business implementation of CCPA and/or GDPR.

What the NY SHIELD Act Adds to California CCPA and EU GDPR Compliance

The NY SHIELD Act has significant similarities to the CCPA and GDPR, including its application to businesses that collect personal information regarding people living in the state, even when the business does not have offices there. And like the GDPR, small businesses are not exempt from the SHIELD Act. Like both the CCPA and GDPR, the SHIELD Act significantly expands the definition of protected "personal information" to include both "any information concerning a natural person which, because of name, number, personal mark or other identifier, can be used to identify such natural person" (emphasis added) and biometric information. General Business Law §899-AA(1)(b). The NY SHIELD Act also expands the definition of data breach to include unauthorized access to private information even when private information was not actually acquired, similar to the CCPA and GDPR. General Business Law §899-AA(3). As with the NY SHIELD Act, under the CCPA and the GDPR businesses have a duty to implement and maintain reasonable security practices and procedures appropriate to the risk presented by the personal information they process. However, unlike the NY SHIELD Act, the CCPA and GDPR do not specify what constitutes reasonable data security. Here's where the benefit of compliance with the NY SHIELD Act really provides value to a business' data privacy and security protection compliance program—by reducing the mystery of compliance and specifying at least some required components of an

effective data security program allowing businesses to be better able to meet 'reasonable data security' for the CCPA and GDPR, as well as the NY SHIELD Act.

Overview of the NY SHIELD Act

The New York SHIELD Act can be found at General Business Law §§899-AA and 899-BB. It requires owners and licensors of computerized data that includes private information concerning New York residents to "develop, implement and maintain reasonable safeguards to protect the security, confidentiality and integrity of the private information, including, but not limited to, the disposal of data." General Business Law §899-BB(2)(a). Entities already compliant with specified federal or state cybersecurity statutes or regulations also satisfy the SHIELD Act. Gramm-Leach-Bliley Act Title V; HIPPA regulations and the Health Information Technology for Economic and Clinical Health Act; New York State Department of Financial Services regulations, 23 NYCRR Part 500; and other federal or state data security requirements. (The last category could be a safe harbor for entities that are federal or state contractors.) Otherwise they must implement a three-part written data security program with both reasonable administrative and technical safeguards, as set out in the law, as well as reasonable physical safeguards, with examples provided in the statute.

Small businesses are not exempt but do get their own test: whether a security program "contains reasonable administrative, technical and physical safeguards that are appropriate for the size and scope of the business activities, and the sensitivity of the personal information the small business collects from or about customers." (Small business is defined in General Business Law §899-BB(1)(c) as (i) a person or business with fewer than 50 employees; (ii) less than $3 million in gross revenue for the last three fiscal years, or (iii) less than $5 million in year-end total assets. It is unclear from the face of the statute whether all three numbered provisions, or only (ii) and (iii), are meant to be disjunctive.) These definitions provide flexibility but the words "reasonable" and "appropriate" can be ambiguous.

Required Notice

The part of the statute already in force before March 21st spelled out the five kinds of access-related information disclosures that are punishable under the law: (1) an account or card number, if that alone is sufficient to access an account; (2) if a password or similar security device is needed to access the account, then an account or card number in conjunction with the password or security code; (3) biometric information; (4) a user name or e-mail which, in conjunction with a password or security code, permits access to a financial account; and (5) HIPPA-related information. The law requires companies to provide notice to New Yorkers when information relating to them was revealed. If the data included information owned by or licensed from another party and private data was or reasonably is believed to have been accessed, that owner or licensor also must be notified of the disclosure "immediately following discovery."

If information relating to more than 500 New Yorkers was revealed, the law requires businesses to notify state officials within 10 days. If officials are not notified, the New

York Attorney General can sue for injunctive relief and actual costs or losses incurred, including consequential damages. Finally, if the violation was knowing or reckless, the court also can award a civil fine of $5,000, or $20 per instance of failure to notify, whichever is greater, up to a ceiling of $250,000.

Importantly, the law's jurisdictional foundation is the disclosure of data "concerning" a New Yorker. As a result, the statute applies to data breaches occurring outside New York if data relating to a New York resident was disclosed. However, the SHIELD Act does not specifically create a private right of action for data disclosure. (These provisions already were in force. Some authors have suggested that monetary remedies under General Business Law §349 could apply. That would permit recovery of actual damages or $50, whichever is larger, with the potential for the court to boost the amount to three times actual damages, not to exceed $1,000, for willful and knowing violations, plus reasonable attorneys' fees. The authors suspect the SHIELD Act was intended to foreclose that option by addressing only actions by the Attorney General.)

No notice is required if the data exposure was accidental and resulted from an authorized user's access to the data, so long as the business "reasonably" determines that misuse of the information, or financial harm, or in some instances, emotional harm, is unlikely. That determination must be documented and kept on file for five years. The statute of limitations is three years from when affected persons were notified or when the Attorney General learned of the breach, whichever is earlier, and in any event, not more than six years. It is very dangerous to try to conceal a breach, because that can mean there is no limitations period.

Courts largely will be writing on a blank slate regarding the SHIELD Act. There are no regulations regarding the statute yet, and the statute does not require any state agency to create them. The repeated use of "reasonable" in General Business Law §899-BB suggests there will be an opportunity to raise and a need to resolve factual disputes as to what was "reasonable" in particular circumstances, with little guidance from the statute. Given the technical nature of the issue, and the likely fluidity of what is "reasonable" in a fast-changing technological field, expert testimony probably will figure prominently in any trial and in pre-trial dispositive motions. Given that courts likely will be writing on a blank slate, it may be wise for entities that later might need to establish the reasonableness of their conduct to follow applicable industry standards.

David Jacoby (djacoby@cm.law) *and* **Linda Priebe** (lpriebe@cm.law) *are partners at Culhane Meadows, PLLC, in its New York and Washington, D.C. offices, respectively. Mr. Jacoby is an adjunct professor of law at Fordham University School of Law. Ms. Priebe is a member of the International Association of Privacy Professionals and holds its CIPP/Europe certification.*

The foregoing content is for informational purposes only and should not be relied upon as legal advice. Federal, state, and local laws can change rapidly and, therefore, this content may become obsolete or outdated. Please consult with an attorney of your choice to ensure you obtain the most current and accurate counsel about your particular situation.

About Culhane Meadows – *Big Law for the New Economy*®

The largest woman-owned national full-service business law firm in the U.S., Culhane Meadows fields over 70 partners in ten major markets across the country. Uniquely structured, the firm's Disruptive Law® business model gives attorneys greater work-life flexibility while delivering outstanding, partner-level legal services to major corporations and emerging companies across industry sectors more efficiently and cost-effectively than conventional law firms. Clients enjoy exceptional and highly-efficient legal services provided exclusively by partner-level attorneys with significant experience and training from large law firms or in-house legal departments of respected corporations. U.S. News & World Report has named Culhane Meadows among the country's "Best Law Firms" in its 2014 through 2020 rankings and many of the firm's partners are regularly recognized in Chambers, Super Lawyers, Best Lawyers and Martindale-Hubbell Peer Reviews.