ALM | LAW.COM

New York Law Journal

Data Breach Liability in New York: What Companies Need to Know

By Stephen L. Brodsky and Branden Lynn

May 18, 2026

In the face of a cyber incident, New York companies may face substantial liability for a data breach—even where the breach originates with a vendor or other third party. Understanding the state's cybersecurity legal framework is therefore critical. That framework is layered, beginning with the Stop Hacks and Improve Electronic Data Security Act (the SHIELD Act), which governs the protection of personal information.

New York also imposes heightened requirements on banks, insurers, and other licensed financial services entities. Sound corporate governance across these regimes is essential, as compliance failures can result in injunctive relief, restitution, and civil penalties. Beyond regulatory exposure, companies may also face civil liability to affected individuals under contract and negligence theories. With the average cost of a data breach reaching $4.88 million in 2024, passive risk tolerance is not a viable strategy.

The SHIELD Act

The SHIELD Act, codified at N.Y. Gen. Bus. Law §§899-aa and 899-bb, is New York's principal data security statute. It applies broadly to any person or business that owns or licenses computerized data containing the private information of a New York resident.

data breach phishing

The statute modernized New York's data breach framework by expanding the definition of a breach to include unauthorized access, extending notification obligations beyond entities doing business in the State, and imposing "reasonable safeguards" requirements calibrated to the size and complexity of the business.

Section 899-bb requires covered entities to develop, implement, and maintain reasonable administrative, technical, and physical safeguards to protect private information. While the statute does not define "reasonable" with precision, guidance from the Attorney General emphasizes identifying foreseeable risks, implementing appropriate protections, and ensuring that service pro-

viders are capable of safeguarding the data they receive. Courts considering analogous statutory schemes have declined to convert regulatory violations into negligence per se where no private right of action exists. See *Smahaj v. Retrieval-Masters Creditors Bureau, Inc*., 69 Misc. 3d 597 (Sup. Ct. N.Y. Cnty. 2020).

A critical feature of the SHIELD Act is its treatment of vendors. The statute imposes a non-delegable obligation on companies to select service providers capable of maintaining appropriate safeguards and to require those safeguards by contract. Responsibility for data security thus extends beyond internal systems to the broader network of third parties that process or store personal information. Although direct case law interpreting this provision is limited, courts in related contexts have emphasized that companies cannot avoid responsibility for entrusted data merely by outsourcing its handling.

If a breach occurs, the SHIELD Act requires notification "in the most expedient time possible and without unreasonable delay," but generally no later than 30 days of discovery. The obligation is triggered where private information "was, or is reasonably believed to have been, accessed or acquired without valid authorization." N.Y. Gen. Bus. Law §899-aa(2).

The statute does not provide a private right of action; enforcement authority rests exclusively with the New York Attorney General. Penalties may include up to $20 per failed notification (capped at $250,000) and up to $5,000 per violation for failure to maintain reasonable safeguards. While a statutory violation does not itself create civil liability, it may be cited as evidence bearing on whether a company met the applicable standard of care.

DFS Cybersecurity Regulation of Financial Services Entities

For financial services companies, the regulatory landscape is more exacting. The New York Department of Financial Services' Cybersecurity Requirements for Financial Services Companies, codified at 23 NYCRR Part 500, impose detailed obligations on covered entities, particularly with respect to third-party risk.

Section 500.11 requires each covered entity to implement written policies and procedures designed to ensure the security of information systems and nonpublic information accessible to, or held by, third-party service providers. These requirements are risk-based and extend beyond initial vendor selection to include due diligence, periodic reassessment, and contractual controls addressing data access, encryption, and breach notification. In this respect, Part 500 adopts a lifecycle approach to vendor risk management.

Regulatory enforcement reflects the seriousness of these obligations. In one recent case, DFS imposed a $4.25 million penalty where the company failed to conduct timely due diligence on vendors before granting them access to sensitive systems. In the *Matter of OneMain Financial Group*, LLC, 2023 WL 7109663 (N.Y. Dep't Fin. Servs. 2023). The enforcement action underscores that vendor onboarding without adequate cybersecurity review—and the failure to revisit vendor risk over time—can itself constitute a regulatory violation. As with the SHIELD Act, Part 500 does not create a private right of action, but violations may carry significant financial and reputational consequences.

Private Civil Exposure

Beyond regulatory enforcement, companies face potential liability in civil actions arising from data breaches, including claims sounding in contract, deceptive practices, and negligence.

Contractual allocation of risk remains a central mechanism for managing exposure. New York courts routinely enforce indemnification provisions that shift data security liability among commercial parties. In *Jetro Holdings, LLC v. MasterCard Int'l Inc*., 166 A.D.3d 594 (2d Dep't 2018), the court enforced a broad indemnification clause requiring a merchant to reimburse an acquiring bank for nearly $7 million in penalties arising from a data breach tied to the merchant's

systems. More broadly, New York courts emphasize that sophisticated parties are bound by their negotiated risk allocations, particularly where the contractual language is clear.

Consumers may also bring claims under N.Y. Gen. Bus. Law §349, which prohibits deceptive acts or practices in consumer-oriented conduct. However, such claims face substantial hurdles in the data breach context. The Court of Appeals has made clear that § 349 requires materially misleading conduct. See *Oswego Laborers' Local 214 Pension Fund v. Marine Midland Bank,* N.A., 85 N.Y.2d 20, 25 (1995).

Applying that standard, courts have consistently rejected claims based on generalized privacy policies. In *Abdale v. North Shore Long Island Jewish Health System, Inc.*, 49 Misc. 3d 1027 (Sup. Ct. Nassau Cnty. 2015), the court held that standard privacy statements do not constitute guarantees against data theft.

Negligence claims present the most nuanced and evolving area of exposure. To state a claim under New York law, a plaintiff must establish a duty of care, breach, and causation. Courts have generally declined to impose a duty to protect against third-party cyberattacks where the defendant lacks control over the compromised system and the harm is not foreseeable. In *Smahaj*, the court dismissed negligence claims arising from a vendor breach, holding that the defendant had no duty to protect plaintiffs from criminal acts targeting systems outside its control.

At the same time, courts have recognized that a duty may arise where a company undertakes to safeguard personal information or makes affirmative representations about its protection. In *Abdale*, the court sustained negligence claims where the plaintiffs alleged that the defendant represented that patient information would not be disclosed without consent. Foreseeability remains the critical factor: allegations of prior breaches, known vulnerabilities, or deficient safeguards may be sufficient to permit a claim to proceed beyond the pleading stage.

Practical Implications

Taken together, New York's statutory, regulatory, and common law frameworks send a consistent message: responsibility for data security extends across the full lifecycle of vendor relationships. Companies cannot treat vendor risk as a purely contractual issue divorced from operational oversight. Rather, vendor selection, onboarding, monitoring, and contractual structuring all inform whether a company has satisfied its obligation to implement reasonable safeguards and, in turn, whether it may face liability in the event of a breach.

Courts will enforce negotiated indemnification provisions, often dispositively reallocating loss, but they will also scrutinize whether a company's public representations about data security align with its actual practices. Generalized privacy statements may not create liability, but specific assurances can. Similarly, while there is no automatic duty to prevent third-party cyberattacks, that analysis shifts where risks are foreseeable or where the company has undertaken responsibility for safeguarding data.

Against this backdrop, companies should adopt a disciplined approach that integrates legal, technical, and contractual controls: implementing rigorous vendor diligence processes, embedding detailed cybersecurity and indemnification provisions into agreements, conducting periodic reassessments, and documenting compliance efforts. In doing so, companies not only reduce regulatory exposure but also position themselves to defend against the increasingly sophisticated civil claims that follow in the wake of a data breach.

Stephen L. Brodsky *is a partner and* **Branden Lynn** *is an associate at Warshaw Burstein.*