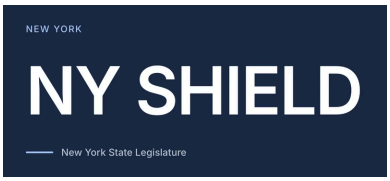
SmartSuite

Framework / Privacy / Global Privacy Regulations

Stop Hacks and Improve Electronic Data Security Act (SHIELD Act), S5575-B, Chapter 117 of the Laws of 2019 (General Business Law sections 899-aa and 899-bb)

The New York SHIELD Act requires any holder of a New York resident's private information to keep reasonable safeguards (GBL 899-bb) and give breach notice within thirty days (GBL 899-aa).



What it is

The New York SHIELD Act (Stop Hacks and Improve Electronic Data Security Act, S5575-B, Chapter 117 of the Laws of 2019) is the state law that requires any person or business that owns or licenses computerized data including the private information of a New York resident to notify affected residents and state agencies of a breach (General Business Law section 899-aa) and to develop, implement and maintain reasonable safeguards for that information (section 899-bb). It was signed on July 25, 2019; the breach notification changes took effect on October 23, 2019 and section 899-bb on March 21, 2020 (section 6 of the act). Since December 21, 2024, when Chapter 647 of 2024 (S2659-B) took effect, notice to residents is due within thirty days of discovery.

At a glance

PUBLISHER
New York State Legislature; enforced by the New York State Attorney General

TYPE
Regulation

VERSION
Chapter 117 of 2019 (S5575-B), as amended by Chapter 647 of 2024 (S2659-B) and later 2025 amendments

EFFECTIVE
October 23, 2019 (breach notification); March 21, 2020 (section 899-bb safeguards); thirty-day notice deadline from December 21, 2024

DOMAIN
Privacy

FAMILY
Global Privacy Regulations

REGION
New York

ADOPTION MODEL
Regulatory Compliance

IMPLEMENTATION COMPLEXITY
Medium

Source: nysenate.gov/legislation/laws/GBS/899-AA

Why it matters

- **A wider definition of private information** Section 899-aa(1)(b) covers biometric information, account numbers usable without a code, and a user name or email address with a password or security question, in addition to Social Security, driver's license and financial account numbers.
- **Access counts as a breach** Section 899-aa(1)(c) defines a breach as unauthorized access to or acquisition of computerized data, with factors for each: viewed, communicated with, used or altered for access; possessed, downloaded, copied or used for acquisition.
- **A thirty-day notice clock** Since Chapter 647 of 2024, section 899-aa(2) requires notice in the most expedient time possible, without unreasonable delay and within thirty days after discovery, subject only to law enforcement needs.
- **Named safeguards** Section 899-bb(2)(b)(ii) lists the administrative, technical and physical safeguards a data security program must include, from a designated coordinator to erasing media at disposal.

 © 2026 SmartSuite Inc. All rights reserved.

How SmartSuite supports NY SHIELD

Section 899-bb Safeguards Library

Load the administrative, technical and physical safeguards in 899-bb(2)(b)(ii) as requirements with a designated coordinator, implementation status, linked policies and evidence, or record the compliant-regulated-entity basis in 899-bb(1)(a).

Risk Identification and Safeguard Assessment

Run the 899-bb(2)(b)(ii)(A)(2) and (3) assessment of reasonably foreseeable internal and external risks and the sufficiency of safeguards as a record, with the network, software, processing, transmission and storage risks the technical safeguards name.

Private Information Inventory

Track in Privacy Management where each category of private information defined in 899-aa(1)(b) is stored, who has access and the disposal schedule 899-bb(2)(b)(ii)(C)(4) requires, including biometric data and online credentials.

Service Provider Oversight

Track each provider's capability review and the contractual safeguards 899-bb(2)(b)(ii)(A)(5) requires in Third Party Risk Management, with review dates and the data categories each provider holds.

Breach Notification Workflow

Run the 899-aa incident record with discovery date, the thirty-day resident deadline, the inadvertent-disclosure determination and its five-year retention, substitute notice thresholds, the notices to the Attorney General, Department of State, State Police and Department of Financial Services, and the consumer reporting agency notice above 5,000 residents.

Control Testing and Monitoring

Record the regular testing and monitoring of key controls, systems and procedures that 899-bb(2)(b)(ii)(B)(4) requires in Cyber & IT Risk, with results linked to the safeguards they test and the program adjustments made after business changes.

Common framework mappings

CIS Controls v8.1 · COBIT 2019 · GDPR · HIPAA · ISO 27001:2022 · ISO 27002:2022 · NIST CSF 2.0 · NIST 800-53 Rev.5 · PCI DSS 4.0.1 · SOC 2

Official resources

State of New York – SHIELD Act (S5575-B) Legislative Text

Provides the full official statute text of the Stop Hacks and Improve Electronic Data Security Act as enacted.

legislation.nysenate.gov/pdf/bills/2019/S5575B

New York State Attorney General – SHIELD Act Compliance Page

Outlines official compliance requirements and breach notification procedures under the SHIELD Act.

ag.ny.gov/resources/organizations/data-breach-reporting/shield-act

New York General Business Law § 899-bb – Data Security Protections

Official text of the SHIELD Act's data security section, which requires reasonable administrative, technical, and physical safeguards for the private information of New York residents.

nysenate.gov/legislation/laws/GBS/899-BB

New York General Business Law § 899-aa – Notification of Breach

Official text of the SHIELD Act's breach notification section, with the expanded definitions of private information and breach of the security of the system.

nysenate.gov/legislation/laws/GBS/899-AA

Frequently asked questions

Who must comply with the New York SHIELD Act?

Any person or business that owns or licenses computerized data including the private information of a New York resident, wherever the business is located; the act removed the earlier requirement to conduct business in New York (General Business Law 899-aa(2) and 899-bb(2)(a)). A business that only maintains such data for its owner must notify the owner of a breach within thirty days (899-aa(3)). Small businesses are covered but scale their safeguards to their size (899-bb(2)(c)).

Updated Oct 15, 2026 · © 2026 SmartSuite Inc. All rights reserved.

What is private information under GBL section 899-aa?

Personal information (anything that identifies a natural person) combined with a Social Security number, a driver's license or non-driver ID number, a financial account or card number with its security code or password, an account or card number usable without one, or biometric information, when the element is unencrypted or the encryption key was also taken; or a user name or email address with a password or security question and answer (899-aa(1)(b)). The current text, as amended through March 28, 2025, also lists medical information and health insurance information. Publicly available government-record information is excluded.

How quickly must a breach be reported, and to whom?

Residents whose private information was accessed or acquired without authorization must be notified in the most expedient time possible, without unreasonable delay and within thirty days after discovery, a deadline added by Chapter 647 of 2024 and effective December 21, 2024 (899-aa(2)). The Attorney General, the Department of State, the Division of State Police and the Department of Financial Services receive the timing, content, distribution, approximate number affected and the notice template (899-aa(8)(a)); consumer reporting agencies are told when more than 5,000 residents are notified (8(b)); a HIPAA covered entity copies the Attorney General within five business days of notifying HHS (9).

What safeguards does GBL section 899-bb require?

Any person or business holding a New York resident's private information must develop, implement and maintain reasonable safeguards to protect its security, confidentiality and integrity, including disposal (899-bb(2)(a)). A data security program is deemed reasonable if it includes administrative safeguards (a designated coordinator, risk identification, safeguard assessment, employee training, service providers selected and bound by contract, and program adjustment), technical safeguards (assessing network, software, processing, transmission and storage risks, detecting and responding to attacks or failures, and regularly testing key controls) and physical safeguards (assessing storage and disposal risks, responding to intrusions, protecting data through collection, transport and disposal, and erasing media so it cannot be read) (899-bb(2)(b)(ii)).

Which businesses are deemed compliant, and what are the penalties?

A compliant regulated entity, meaning a business subject to and compliant with the GLBA Title V regulations, the HIPAA and HITECH regulations, 23 NYCRR Part 500 or other federal or New York data security rules, is deemed to meet the safeguards duty (899-bb(1)(a) and (2)(b)(i)). For notification failures the Attorney General may seek an injunction, damages for persons not notified and, for knowing or reckless violations, a civil penalty of the greater of $5,000 or up to $20 per failed notification, capped at $250,000 (899-aa(6)); a safeguards failure is a violation of GBL section 349, for which the Attorney General's SHIELD Act page cites a penalty of up to $5,000 per violation (899-bb(2)(d)). There is no private right of action (899-bb(2)(e)).

License included / downloadable: Yes The SHIELD Act and the General Business Law sections it amended are New York State laws published free by the New York State Senate and the Attorney General; the platform links to the official text.

Full framework page and mappings: smartsuite.com/frameworks/us-new-york-shield-act-s5575b-stop-hacks-improve-electronic-data

© 2026 SmartSuite Inc. All rights reserved.