SHIELD Act (NY) Overview

Summary

The Stop Hacks and Improve Electronic Data Security (SHIELD) Act is a New York state law (S.5575-C/A.5578-C, signed July 25, 2019) that amends the state's 2005 data breach notification law to strengthen protections for residents' private information. Effective March 21, 2020 (with December 2024 amendments adding a 30-day notification timeline and the Department of Financial Services to reporting), it expands the definition of breaches, broadens territorial scope, and mandates data security safeguards. Administered by the New York Attorney General (AG), it aims to prevent data misuse by requiring proactive security and timely breach responses, without a private right of action but allowing AG enforcement. Non-compliance can lead to injunctive relief, restitution, and civil penalties. (Clarification: Penalty amounts are not specified in the law and are determined by the NY Attorney General.)

Key Requirements

The SHIELD Act focuses on data security programs and breach notification. Key requirements include:

1. **Data Security Safeguards**:
    - Any person or business owning or licensing computerized data with New York residents' private information must develop, implement, and maintain reasonable administrative, technical, and physical safeguards to protect its security, confidentiality, and integrity.
    - For small businesses: Safeguards appropriate to size, complexity, and data sensitivity.
    - Deemed compliance if adhering to standards like GLBA Safeguards Rule, HIPAA Security Rule, NY DFS Cybersecurity Regulation (23 NYCRR 500), or other federal/state data security rules.
2. **Definition of Private Information and Breach**:
    - **Private Information**: Personal info (name + SSN, driver's license/ID number, account/credit/debit card number) plus new elements: financial account numbers, biometric info, email addresses with passwords/security questions/answers.
    - **Breach**: Unauthorized acquisition or access (not just acquisition) compromising security, confidentiality, or integrity; includes unencrypted/compromised encrypted data.
3. **Breach Notification**:
    - Notify affected individuals without unreasonable delay and in the most expedient time possible, subject to law enforcement needs; 2024 amendment caps at 30 days.
    - Notify NY AG, Department of State, and State Police via AG's portal (includes timing, content, distribution, affected count, and notice copy).
    - If >5,000 residents affected, notify major credit reporting agencies (e.g., Equifax).

    - No notification if exposure unlikely to cause misuse, financial/emotional harm, or if good-faith info security procedures were followed; document determination (retain 5 years; submit to AG if >500 affected, within 10 days).
    - Substitute notice allowed if direct notice costs >$250,000, affects >500,000 residents, or email unavailable (e.g., conspicuous website posting, media notice).
    - Include contact info for notifier and resources for identity theft prevention/security breach response.
4. **Data Disposal**:
    - Dispose of private information securely (e.g., shredding, erasure) to prevent recovery by unauthorized parties.

Compliance Process:

- Conduct risk assessments, employee training, vendor oversight, and timely disposal.
- Document all breaches and security measures for potential AG review.
- No mandatory audits, but AG can investigate violations.

2025 Context: The December 2024 amendments (effective immediately) enhance notification timelines and reporting, aligning with national trends for faster breach responses.

Who Is Affected

- **Persons or Businesses**:
    - Any entity (regardless of location) that owns or licenses computerized data containing private information of New York residents (e.g., companies collecting/processing NY data via websites, apps, or services).
    - No size threshold; applies to all, including small businesses (with scaled safeguards).
- **Residents (Data Subjects)**:
    - New York residents whose private information is exposed, entitled to timely notification and resources for harm mitigation.
- **Employees and Vendors**:
    - Staff handling private information must receive training; third-party vendors (e.g., IT providers) must align with safeguards via contracts.
- **Regulators**:
    - NY AG enforces via investigations; notifications go to AG, Dept. of State, State Police, and Dept. of Financial Services (per 2024 update).
- **Impact of Non-Compliance**:
    - AG remedies: Injunctive relief, restitution, civil penalties (amounts not specified, but tied to unfair practices).
    - Reputational damage; no private lawsuits, but overlaps with other laws (e.g., negligence claims).

Informational Resources

- **NY AG SHIELD Act Page**: ag.ny.gov/resources/organizations/data-breach-reporting/shield-act (official guidance, breach reporting portal, FAQs).
- **NY State Legislature Text**: nyassembly.gov/leg/?default_fld=&leg_video=&bn=A05578&term=2019&Summary=Y&Text=Y (full bill text, amendments).
- **NY DFS Cybersecurity Resources**: dfs.ny.gov/industry_guidance/cybersecurity (aligns with deemed compliance under 23 NYCRR 500).
- **Training and Tools**:
  - NY AG Webinars: ag.ny.gov (free sessions on breach notification and safeguards).
  - IAPP SHIELD Act Guide: iapp.org/resources/article/ny-shield-act (paid membership for detailed compliance tools).
  - Osano SHIELD Act Toolkit: osano.com/articles/new-york-shield-law (free checklists, templates).
- **Industry Resources**:
  - PwC SHIELD Act Summary: pwc.com/us/en/services/consulting/cybersecurity-risk-regulatory/library/new-york-shield-act.html (free overview, compliance tips).
  - Willkie Compliance Concourse: complianceconcourse.willkie.com/resources/privacy-and-cybersecurity-us-new-york-shield-act-overview (free analysis, updates).
  - Usercentrics Guide: usercentrics.com/knowledge-hub/new-york-shield-act (free explainer, 2024 amendments).
- **Community Support**:
  - IAPP Privacy Community: iapp.org/connect (forums for NY privacy pros).
  - Privacy Rights Clearinghouse: privacyrights.org (consumer-focused breach resources).