# SHIELD Act Notice Starts With Technical Facts

The SHIELD Act requires notice to affected New York residents within 30 days of discovering a breach, and the notice list rests on the technical facts. Who accessed what, through which identity and during which period is a forensic question first. This note shows how to build those facts quickly and defensibly.

Edition 2026-11-03 · Online at newyorkcomputerforensics.com/insights/new-york-shield-act-incident-facts/

The 30 day notice rule is in New York General Business Law section 899-aa, and the technical facts have to be ready well inside it. The sections below show how to separate a system compromise from supported findings about data access, and how to keep the safeguards and response decisions on record.
The SHIELD Act changed New York's data breach and reasonable safeguard framework. Responders should preserve the facts needed for that decision while containment and recovery are still underway.

## Distinguish System Compromise From Supported Access Findings

A compromised account or host establishes risk, and access to particular records is examined record by record. Analysts identify the affected identity, privileges, systems, data stores, queries, file events, mailbox activity, transfer methods, staging, exfiltration indicators, and log coverage. The report states where evidence supports access and where it supports acquisition, and it names the telemetry each conclusion rests on.

## Prepare Source Records for the Notice Decision

If data was accessed, the team identifies the repositories, record types, fields, affected period, ownership, deduplication method, encryption state, and confidence in the count. Assumptions are listed. Reconciliation turns a preliminary estimate into the final population.

Coverage includes initial access, persistence, privilege, and activity window; affected systems, repositories, backups, and synchronized copies; personal information fields present in the accessed material; evidence of viewing, querying, staging, transfer, or deletion; and known logging gaps and steps taken to validate them.

## Preserve Safeguards and Response Decisions

Keep the relevant policies, technical controls, risk records, access reviews, vulnerability findings, training evidence, vendor terms, alert history, response chronology, and corrective actions. Those materials reflect the environment at the time.

## Primary Sources and Technical References


- New York Attorney General, SHIELD Act https://ag.ny.gov/resources/organizations/data-breach-reporting/shield-act


© 2026 Global Digital Forensics, Inc. All rights reserved.

## Get Incident Help Now

Call the 24/7 hotline now if an incident is under way. A responder will help contain it and preserve the records your response depends on, and the first consultation is free. Requests are handled in confidence.

**Call (800) 868-8189, 24/7 · New York office (212) 561-5860**

Email info@evestigate.com or request your consultation at newyorkcomputerforensics.com/contact.

© 2026 Global Digital Forensics, Inc. All rights reserved.