Global Digital Forensics · Guide edition 2026-11-03 · evestigate.com/insights/new-york-shield-act-incident-facts/

ENTERPRISE BREACH EVIDENCE

Scoping New York SHIELD Act Notification From the Data Record

Under the SHIELD Act unauthorized access alone can trigger notification, and the examiner's reading of which items an intruder touched is what counsel uses to size the notice to the facts. Preserve the logs before they roll and route the analysis through counsel. Call (800) 868-8189 at any hour.

Published September 5, 2026 · Updated October 30, 2026

By Joseph Caruso, Founder, CEO and CTO, Global Digital Forensics

Why the SHIELD Act Access Trigger Calls for Granular Evidence

Unlike older state data breach statutes that only triggered notification duties when personal information was provably acquired or downloaded, the New York SHIELD Act broadened the definition of a breach to include unauthorized access to computerized data containing private information, including viewing, communicating or altering records. When an attacker compromises an employee email account or a network file server that houses tens of thousands of customer records, granular forensic telemetry is what lets an organization measure what the intruder actually viewed, in place of assuming every file in the repository was reached, with the notification costs, regulatory scrutiny from the New York Attorney General and class action exposure that assumption brings.

Using Forensic Telemetry to Measure What the Intruder Touched

Operating directly under the direction of retained privacy counsel, Global Digital Forensics performs precise data access reconciliation engagements that separate theoretical repository exposure from actual unauthorized access. Across Microsoft 365 environments, file servers and cloud databases, our examiners correlate Microsoft Purview MailItemsAccessed events, SMB network share logs, NTFS Master File Table access records, egress firewall traffic volumes and archive creation artifacts. Where the record shows that an intruder accessed a specific subfolder or searched for specific wire transfer keywords, leaving human resources and customer identity files unopened, we help the legal team narrow notification populations and support that determination before regulators.

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

The Statute's Own Words and the Factors the Attorney General Weighs

General Business Law section 899-aa, as amended by the SHIELD Act, defines a breach of the security of the system to include unauthorized access to or acquisition of computerized data that compromises the security, confidentiality or integrity of private information. The statute then tells the organization how to decide whether access occurred: it may consider indications that the information was viewed, communicated with, used or altered by a person without valid authorization. Those four verbs are the vocabulary of the technical record. A mailbox item bound by an attacker's session was viewed. A file copied through an SMB share was used. A forwarding rule that pushed messages to an outside address means information was communicated with. An examiner's job is to map the artifacts onto that language so the lawyers can apply it.

Timing is set in the same section. Notice to affected residents must be made in the most expedient time possible and without unreasonable delay, and in no event later than 30 days after the breach is discovered, unless a law enforcement agency determines that notice would impede a criminal investigation. Those 30 days are the window in which forensic reconciliation happens, and regulators will ask how long it took and why. The same section requires notice to the Attorney General, the Department of State and the Division of State Police, and a business that is a covered entity under 23 NYCRR 500.1 also notifies the Department of Financial Services, in the manner 23 NYCRR 500.17 sets. The Attorney General's SHIELD Act page describes the reporting form and the private information categories, which include online account credentials, biometric data, medical information and health insurance information as well as Social Security, driver's license and financial account numbers. We build the analysis around those categories so the population reported to regulators matches what the record supports.

Reading a Compromise Against the Access Standard

In a Microsoft 365 tenant the central artifact is the MailItemsAccessed operation in the unified audit log, which records bind and sync access to mailbox items with the session identifier, client application and IP address that performed it. Correlating those entries with the attacker's sign in sessions from Entra ID separates what the account owner did from what the intruder did. Sync access tells us a client pulled a folder in bulk, bind access tells us individual items were opened, and the throttling indicator flags the periods when high volume caused the log to aggregate items. Inbox rules, OAuth application consents, eDiscovery searches and SharePoint file access events fill in the rest. The result is a documented list of the items recorded against the attacker's sessions, which is what the viewed and used factors call for.

On a Windows file server the equivalent record comes from object access auditing, SMB share events, the NTFS Master File Table and the USN change journal, together with any archive files the intruder created to stage data and the egress volumes recorded at the firewall. We also state clearly how each record is read. Mailbox auditing records access for mailboxes where it was enabled and licensed, so the examiner confirms that setting first. A bound message records that the item was opened, and the content review of that item shows what it held. Volume at the firewall measures how much left, and the examiner looks for the staged archive to learn what it contained. The coverage of every source is documented before anyone decides the population, and our compromise analysis reports are written to make that coverage explicit.

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

Google Workspace and other platforms keep their own versions of the same record. Workspace audit logs record Gmail access events, Drive file views and downloads and the OAuth tokens granted to third party applications, and the login audit shows sessions by address and device. File sharing platforms record previews, downloads and link creation with the account and address that performed them. The analytical question is the same on every platform: which sessions belonged to the intruder, what did those sessions touch and does the platform record touching at the level of the individual item. Where it records item level access, the population can be narrowed to the items. Where it records folder or repository level access, the notification analysis works at that level, and we confirm which applies before the analysis begins.

How the Data Reconciliation Engagement Proceeds

The engagement begins with a scoping call, held under the privacy attorney's direction, that identifies the compromised accounts, servers or applications, the licensing and audit configuration of the tenant and the retention windows that are running. Preservation comes first: the unified audit log, sign in logs, mailbox audit records and server event logs are exported with their native timestamps while they are within retention, and the mailbox or share itself is preserved so the items referenced in the logs can be examined. We ask IT to keep the account, the rules and the server as they are until that export is complete, because those are the entries the examiner reads to narrow the population.

Analysis then proceeds in two directions. We reconstruct the intruder's sessions and the items they touched, and we examine those items for private information as the statute defines it, which is the sensitive content assessment that turns a list of message identifiers into a list of affected individuals. The legal team receives the reconciled population with the artifacts behind every inclusion and exclusion, so the notification decision rests on records rather than on an assumption that the entire repository was exposed. If the Attorney General or another regulator asks how the population was determined, the same examiner can answer in a declaration or in person. Our privacy incident technical support work is structured for exactly that follow up.

The report has a defined shape. It opens with the scope and the sources examined, states the audit configuration and retention that bounded the analysis, reconstructs the intruder's sessions with timestamps and identifiers, lists the items touched with the artifact behind each and presents the population of individuals whose private information sat in those items by category. A separate section sets out each question the sources left open, the sources checked for it and the reason. Attorneys use that structure directly in the notice to the Attorney General and in responses to regulator questions, and when a class action follows, the same report supports a declaration from the examiner who performed the work. Writing to that standard from the start is faster than rewriting a technical memo into a defensible record later.

Steps That Keep the Notification Population Accurate

The most valuable step is exporting the record while it is within retention. Unified audit log and sign in log retention is finite and varies by license, so engaging an examiner early captures whatever the logs still hold of the attacker's sessions. Keeping the compromised account and the file server intact until the export is done serves the same purpose. Containment reaches past the password reset to the OAuth tokens and application consents that survive it. The population rests on the record rather than on the attacker's claim about what was taken, in either direction. Our guide to the first hours of a business email compromise lays out the order of operations that keeps each of these steps on track.

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

Who acts before the first call matters as much as what is done. General counsel engages privacy counsel and routes the technical work through that engagement. The Microsoft 365 or Google Workspace administrator confirms audit status and begins the exports, or at minimum pauses any process that would remove records. The data owner for the affected repository describes what categories of private information it holds, so the sensitive content assessment can be scoped. Human resources and finance identify whether employee or customer records sit in the mailboxes involved. Our New York private information records package lists these roles and the documents each should gather, and our cloud forensics team handles tenants beyond Microsoft.

Protecting Your SHIELD Act Timeline

Because cloud and network access logs overwrite rapidly, engage technical examiners through your attorneys immediately upon discovering an intrusion. Our New York private information records package lists what the legal and IT teams should gather first.

Call Global Digital Forensics at (800) 868-8189 or our New York office at (212) 561-5860 to initiate a SHIELD Act technical assessment. The initial consultation is free.

The Access Factors Mapped to the Technical Record

The SHIELD Act tells an organization it may consider whether information was viewed, communicated with, used or altered without authorization. This table maps each of those verbs onto the artifact that speaks to it and states how the examiner reads that artifact, so the statute's own language can be applied to the record. The third column guides the narrowing of a notification population: a bound message records that an item was opened, and the content review shows what that item held. Where a mailbox was never audited, the examiner records the setting and works from the content the session could reach.

SHIELD Act access factors, the artifact that addresses each and how the examiner reads that artifact.

Statutory factor	Artifact that addresses it	How the examiner reads it
Viewed	MailItemsAccessed bind events in the audit log	An item was opened; the content review shows what it held
Communicated with	Forwarding rule or external send events	The rule itself; its creator is checked against the sign in sessions
Used	SMB share access, file copy and download events	Access and copying; the examiner looks for later handling on the receiving device
Altered	USN change journal and object access auditing	Changes on volumes where auditing was enabled, confirmed first
Which session	Entra sign in logs by address, device and method	The infrastructure behind a session; tying it to a person adds corroboration
How much left	Egress volume at the firewall	Volume; the examiner looks for content in packet capture or the staged archive
Private information present	A sensitive content assessment of the touched items	Read from the touched items, preserved for review

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

The insurance company examination shows how reconciling records across sources let regulators separate what the systems actually showed from what was assumed, the same discipline this guide applies to a notification population.

How to Begin and What Happens on the First Call

Have at hand the accounts or systems you believe were compromised, the date the activity was noticed, the licensing tier and audit status of your tenant, and a description of the kinds of personal information the affected repositories hold. Our examiner asks whether the account has been contained, whether exports have started, what retention windows are running and whether a privacy attorney is engaged, because the work proceeds under that attorney's direction. You then receive a written scope describing the preservation steps, the reconciliation method, a timing plan keyed to the statute's expectation of no unreasonable delay and a proposal for the final report. The initial consultation is free, and the hotline at (800) 868-8189 is answered 24/7, with our New York office at (212) 561-5860 during business hours.

Technical References and Further Reading

Primary sources and provider documentation behind this guide: New York Attorney General: SHIELD Act.

Authorities cited in this guide: New York General Business Law section 899-aa. Supplies the SHIELD Act definitions of breach, private information and the access factors, and the notice timing language quoted in this guide, in the current consolidated text on the Senate site. New York Attorney General, SHIELD Act data breach reporting. Describes the Attorney General's reporting form and the information categories covered, as published on the current Attorney General resource page. NIST SP 800-86. Provides the forensic process model for collecting and examining logs and systems that underlies the reconciliation method, in the final published version.

FREQUENTLY ASKED

Viewed Records, Timing and Cost Under the SHIELD Act

Does the SHIELD Act require notification if the attacker only looked at the data?

It can. The statute defines a breach to include unauthorized access, not only acquisition, and it directs the organization to consider indications that information was viewed, communicated with, used or altered. Whether a particular file or message was viewed is a factual question the examiner reads the audit record to answer. The forensic work is what lets counsel apply the statute to actual access events rather than to the whole repository. Where the record shows the intruder's sessions stayed away from the records holding private information, the legal team has a basis to conclude those individuals were unaffected.

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

How long does a SHIELD Act access reconciliation take?

The drivers are the number of compromised accounts or systems, whether mailbox auditing was enabled, the size of the repository the intruder could reach and how quickly we receive exports. A single compromised mailbox with full audit coverage reconciles fastest, and a file server where object access auditing was off takes longer, because the examiner draws on the Master File Table, the USN change journal and egress records instead. The statute requires notice without unreasonable delay and within 30 days of discovery, so we begin preservation on the first day and report in stages as the population firms up.

What does the engagement cost?

The initial consultation is free. The proposal that follows reflects the number of accounts and systems involved, the state of the logging, the volume of items that need sensitive content assessment and whether the matter needs a declaration or testimony beyond the technical report. Narrowing a notification population from an entire repository to the items actually accessed usually costs far less than notifying, credit monitoring and defending a population that was never touched.

Can you tell us what the attacker read in a message they opened?

The audit record notes that an item was bound or synced by the attacker's session, which supports the conclusion that it was accessed, and the content review shows what the item held. We examine the content of each accessed item for the private information categories the statute names, so it is clear which individuals' data was in the items the intruder reached. That combination is what supports a well founded population.

Should we reset the password before calling a forensic examiner?

Contain the account right away, in a way that preserves the record. Reset the password, revoke sessions and tokens, and screenshot or export suspicious inbox rules and application consents before removing them. Keep the account and the mailbox in place. Begin the audit log and sign in log exports immediately, so whatever the logs hold of the attacker's sessions is captured within retention. Then call, and we will confirm what else to preserve.

Web Addresses for the Sources Cited

1. unauthorized access to or acquisition of: https://www.nysenate.gov/legislation/laws/GBS/899-AA
2. Attorney General's SHIELD Act page: https://ag.ny.gov/resources/organizations/data-breach-reporting/shield-act
3. NIST SP 800-86: https://csrc.nist.gov/pubs/sp/800/86/final

Reviewed by Joseph Caruso, Founder, CEO and CTO, CISSP. Last reviewed November 3, 2026.

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

Start With a Free Consultation

The initial consultation is free, and requests are handled in confidence. On the first call a senior member of our team listens to the question you need answered, identifies the records and systems involved, and recommends the next step.

Call (800) 868-8189, answered 24/7, request a consultation at evestigate.com/contact, or email info@evestigate.com.

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