Greater N.Y. Mut. Ins. Co. v SKOUT Monitoring, LLC
2026 NY Slip Op 31354(U)
April 2, 2026
Supreme Court, New York County
Docket Number: Index No. 650539/2022
Judge: Joel M. Cohen
Cases posted with a "30000" identifier, i.e., 2013 NY Slip Op 30001(U), are republished from various New York State and local government sources, including the New York State Unified Court System's eCourts Service.
This opinion is uncorrected and not selected for official publication.

SUPREME COURT OF THE STATE OF NEW YORK
COUNTY OF NEW YORK: COMMERCIAL DIVISION PART 03M

----------X

GREATER NEW YORK MUTUAL INSURANCE COMPANY,

Plaintiff,

- v -

SKOUT MONITORING, LLC, CONSOLIDATED TECHNOLOGIES, INC.,

Defendants.

INDEX NO. 650539/2022

MOTION DATE 03/10/2025, 07/03/2025, 07/03/2025

MOTION SEQ. NO. 010 012 013

DECISION + ORDER ON MOTION

----------X

HON. JOEL M. COHEN:

The following e-filed documents, listed by NYSCEF document number (Motion 010) 370, 371, 372, 373, 374, 375, 376, 377, 378, 379, 380, 381, 382, 383, 384, 385, 386, 387, 388, 389, 390, 391, 392, 393, 394, 395, 396, 397, 398, 399, 400, 401, 402, 405, 406, 407, 408, 409, 410, 411, 412, 413, 414, 415, 416, 417, 418, 419, 420, 421, 422, 423, 424, 425, 426, 427, 428, 429, 430, 431, 432, 433, 434, 435, 436, 437, 438, 439, 440, 446, 454, 455, 456, 482, 483, 484, 485, 486, 487, 488

were read on this motion for SPOLIATION SANCTIONS.

The following e-filed documents, listed by NYSCEF document number (Motion 012) 458, 459, 460, 461, 462, 463, 469, 470, 471, 472, 528, 529

were read on this motion to PRECLUDE.

The following e-filed documents, listed by NYSCEF document number (Motion 013) 464, 465, 466, 467, 468, 473, 474, 530, 531

were read on this motion to PRECLUDE.

Plaintiff Greater New York Mutual Insurance Company ("GNY") moves pursuant to CPLR 3126 for spoliation sanctions, including striking Defendant SKOUT Monitoring, LLC's ("SKOUT") Answer or, alternatively, an adverse inference and an award of attorneys' fees and costs.

For the reasons set forth below, and after conducting an evidentiary hearing, the Court concludes that SKOUT's failure to preserve relevant (and potentially material) evidence while

litigation was reasonably anticipated and even while litigation was actually pending constituted grossly negligent spoliation. Taking into account the relevant facts and circumstances, the Court determines that an appropriate sanction is an adverse inference that the spoliated evidence would have supported GNY's claims, as well as awarding GNY compensation for its reasonable attorneys' fees and costs incurred in connection with this motion and the evidentiary hearing. The Court declines to strike SKOUT's Answer.

BACKGROUND

This action arises from a ransomware attack on GNY's computer systems between May 19, 2021 and June 1, 2021 (NYSCEF 3 ¶¶ 3, 26, 33; DX-8 at 6; DX-9 at 1). GNY alleges that SKOUT, its security operations center provider, failed to properly monitor GNY's systems and notify the company of malicious activity preceding the cyberattack (NYSCEF 3 ¶ 33).

As described in greater detail below, SKOUT's monitoring systems generated and recorded in real time data and internal communications reflecting and regarding activity within GNY's network, including alarms, alerts, internal communications, and ticketing records documenting SKOUT analyst review and incident response (Khan Aff ¶¶ 7–11). That information was maintained across multiple platforms, including Slack (internal communications), Elastic (historical alarm data), and Zendesk (ticketing and analyst disposition records) (PX-42 at 8–11; NYSCEF 485, July 7 Hearing Transcript ["July 7 tr"] 72:10–21). As GNY contends, these categories of electronically stored information capture, among other things, SKOUT's contemporaneous awareness of and response to suspicious activity preceding the ransomware attack and are therefore relevant and potentially material to its claims (*see* NYSCEF 482).

In August 2024, GNY moved for spoliation sanctions, citing SKOUT's failure to preserve and produce Slack communications, tickets, alarms, and alerts related to the cyberattack (NYSCEF 188, August 2, 2024 First Motion for Sanctions at 8). By Decision and Order dated September 13, 2024, the Court denied the motion without prejudice due to disputed questions of fact that needed to be resolved at an evidentiary hearing or at trial (NYSCEF 244). The Court directed SKOUT to determine whether a database containing GNY-related alarms and alerts existed and, if so, to make it accessible to GNY (NYSCEF 249, September 13, 2024 Hearing Transcript at 64-69).

Following the September 2024 hearing, SKOUT represented that it had located in its Elastic database alarms and alerts that were generated between May 19, 2021 and February 3, 2022, (JX-39 at 61). Upon inspecting the database on January 29 and February 13, 2025, GNY discovered that it was incomplete because historical alarms and alerts predating the cyberattack were missing (Cole Aff ¶ 50).

On March 10, 2025, GNY filed its second motion for spoliation sanctions, asserting that SKOUT failed to preserve and produce (i) Slack communications from May and June 2021; (ii) Slack communications from July 2021 through February 3, 2022; (iii) historical alarm data predating May 19, 2021 (the date when the cyberattack began) stored in SKOUT's Elastic database; and (iv) ticket data from Zendesk (JX-12; JX-15).

By Decision and Order dated April 30, 2025, the Court directed an evidentiary hearing to resolve three issues of fact: (1) when SKOUT's duty to preserve arose; (2) the relevance of the information at issue; and (3) whether that information was requested during discovery (NYSCEF 446). During the evidentiary hearing, which was held on July 7, 2025, the Court heard testimony

from fact and expert[1] witnesses (*see* NYSCEF 485, July 7 tr) and received documentary evidence, including affidavits,[2] exhibits, and system records. The parties thereafter submitted post-hearing briefs addressing the factual issues identified by the Court (*see* NYSCEF 482, 489).

Based on the evidence presented and the parties' submissions, the Court makes the following findings of fact and conclusions of law with respect to spoliation.

FINDINGS OF FACT

I. SKOUT's Obligations Under the Aegis Agreement

In 2017, GNY retained SKOUT as its cybersecurity provider pursuant to the Aegis Platform Services Agreement[3] ("Aegis Agreement") (JX-1). Under the Aegis Agreement, SKOUT agreed to perform "24/7/365 Monitoring" on GNY's computer networks and "Early Warning Threat Detection & Analysis" whereby SKOUT's "Real-Time Data Analysts" would provide "expert level network, security and cyber intelligence" to "identify, notify, and remediate threats" (*id*. at 9).

In the ordinary course, SKOUT performed its monitoring services by using its Security Information and Event Management ("SIEM") system to ingest logs capturing activity within

[1] SKOUT's motion to preclude the testimony of GNY's expert, Eric Cole, PhD (Mot. Seq. 12), is denied. SKOUT argues that Dr. Cole's July 1, 2025 affidavit exceeded prior disclosures and was untimely. CPLR 3101(d) requires disclosure of expert opinions in reasonable detail, and preclusion rests in the Court's discretion (*Rivera v Montefiore Med. Ctr.*, 28 NY3d 999, 1002 [2016]). The Court finds no material deviation from prior disclosures and no prejudice warranting preclusion.

[2] SKOUT's motion in limine to preclude certain witness affidavits and exhibits (Mot. Seq. 9) is denied. SKOUT argues that the challenged materials exceed the scope of the Court's April 30, 2025 Order directing a targeted evidentiary hearing (NYSCEF 446). The Court finds that the challenged materials bear on when litigation was reasonably foreseeable and thus on the timing of SKOUT's preservation duty, and any specific objections were addressed at the hearing.

[3] The contract was entered into by SKOUT's predecessor, Oxford Solutions Analytics, LLC (JX-1).

GNY's network and compare them against "use cases," predefined specific security threats, such as repeated failed login attempts or access from an unusual location (Ok Aff ¶ 33; Khan Aff ¶ 7). When a use case was triggered, SIEM generated alarms reflecting potentially suspicious activity detected within GNY's network (*id.*). Those alarms were then routed to Zendesk, SKOUT's customer service and ticketing platform, where cybersecurity analysts reviewed the alarms and determined whether they warranted notifying GNY (PX-42 at 8–11; July 7 tr 35:19–23, 72:11–18). Alarm data generated by SIEM was stored in two systems: FortiSIEM and Elastic, a backup system containing historical alarms and alerts data; corresponding tickets documenting analyst review and disposition were maintained in Zendesk **(**July 7 tr 69:19–21, 72:19–21; Kannan Aff ¶¶ 6–7**)**.

II. SKOUT's Prior Emphasis on Evidence Preservation

Among the services SKOUT provided to GNY was an analysis and update to GNY's existing incident response plan. In March 2019, SKOUT conducted a real-world cyber incident simulation to guide GNY through incident response procedures (PX-39 [Data Protection & Security Breach Readiness Overview]). As part of that exercise, SKOUT emphasized the importance of document preservation in the aftermath of a cyberattack, instructing GNY to "[d]ocument everything" because "[m]emory is not sufficient" (*id*. at 22). This guidance reflects SKOUT's recognition that accurate documentation and preservation of system activity and response measures are critical following a cyber incident.

III. The Ransomware Attack

As alleged by GNY, on May 19, 2021, a cybercriminal group known as "PYSA" launched a brute force attack[4] on GNY's computer system, making over 910,000 failed login attempts utilizing various combinations of usernames and passwords to access the system (DX-8 [Incident Response and Forensic Analysis Report by PocketWatch] at 11–12). On or around May 25, 2021, PYSA succeeded in gaining access to GNY systems (*id*.; JX-4 [June 1, 2021 Correspondence from SOC to Code Orange]). On May 31, 2021, PYSA deployed ransomware that crippled GNY's networks and operations (*id*.).

GNY alleges that SKOUT failed to alert GNY of the extensive suspicious activity on GNY's systems at any time in the lead-up to—or during—the ransomware attack (Ok Aff ¶ 41). SKOUT sent one "medium" risk ticket at 11:39 p.m. on May 31, 2021 regarding an incident that occurred at 11:27 p.m. that same night (JX-2 at 2). The ticket noted that SKOUT detected "multiple (more than 3) accounts were disabled . . . within [GNY's] network in a short period of time" (*id*.). GNY, however, never received the ticket because its email system had already been blocked by the cyberattack (*id*. ¶¶ 42, 45; JX-7 [June 2-3, 2021 Email chain between Russo and Khan] at 3–8).

IV. The Aftermath of the Ransomware Attack

On June 1, 2021, GNY informed SKOUT that its systems were compromised by ransomware (JX-4 [June 1, 2021 Correspondence from SOC to Code Orange]). Later that day, GNY made repeated requests for historical logs of GNY's systems that were in SKOUT's

[4] A "brute force" attack involves a would-be malefactor repeatedly using trial and error to obtain unauthorized access to a computer system (*Greater New York Mut. Ins. Co. v Skout Monitoring, LLC*, 2022 N.Y. Slip Op. 33575[U], 4 [N.Y. Sup Ct, New York County 2022]).

possession so that GNY (and the digital forensics team it retained) could analyze the cyberattack and restore the network (*id*. at 2–3; PX-36 [June 2, 2021 email from J. Ok to D. Schelmay]). SKOUT asserts that it provided GNY with more than 400 system logs related to the ransomware attack (Khan Supp Aff ¶ 28).

Upon learning of the cyberattack, a senior incident response and attack analyst from SKOUT began an initial investigation into the cyberattack (JX–4 at 2; JX-5; Khalid Aff ¶¶ 11, 14). On June 2, 2021, the analyst shared her incident response notes and summary of the initial investigation with the vice president of SKOUT's Cyber Intelligence Center (Khalid Aff ¶14; JX-5). The analyst discovered that tickets for GNY were mis-mapped, alerts regarding suspicious activity were incorrectly routed to the wrong client, and SKOUT received over 500 brute force alarms associated with GNY that were closed out as "failed attempts" (JX-5).

On June 10, 2021, shortly after the GNY event, SKOUT held an internal "All Hands" meeting. In that meeting, the May 31, 2021 ticket—which GNY never received—was cited as an example of a "big red flag" that "should not be de-escalated" and that "needs to be sent as a high and the customer needs to see":

> And this is one example where this ticket came in at off-hours on a holiday and it was four accounts disabled. Which, in itself should be a big red flag, right? Thinking as a security analyst, as a security professional, you know, when it's, you know, midnight and four accounts get disabled, this is something that need -- that should not be deescalated. That needs to be sent as a high and the customer needs to see -- receive the call. In this case, the customer didn't see it and they actually ended up having an active ransomware infection. So, that's how you have to think, like, that's what's at stake.

(NYSCEF 486 at 3:9–22).

V. Auto-Deletion of Slack Communications

SKOUT analysts used Slack for written internal communications during the period of the cyberattack against GNY (July 7 tr 30:15–31:1; PX-4 83:10–84:17). SKOUT maintained a 30-

day retention policy for Slack, which was not suspended after the ransomware attack or after GNY's December 16, 2021 preservation demand letter discussed below (Khan Aff ¶31). As a result, internal Slack messages from May–June 2021 relating to the GNY attack were not retained (*id*.).

VI. GNY's December 16, 2021 Demand Letter

On December 16, 2021, GNY sent SKOUT a letter demanding, in part, preservation of documents and attaching a draft complaint (JX-22). Senior SKOUT executives maintain that SKOUT's duty to preserve documents arose on December 16, 2021 and that they did not believe GNY contemplated litigation against SKOUT prior to that date (Khan Aff ¶ 33; Russo Aff ¶¶ 11–12). As discussed *infra*, however, the Court finds that a reasonable anticipation of litigation arose (or should have arisen) in the immediate aftermath of the ransomware attack in early June 2021 based on SKOUT's internal investigation and identification of substantial suspicious activity prior to the attack that had not been reported to GNY.

Other than an email from SKOUT's general counsel forwarding GNY's demand letter to a senior employee, SKOUT never instituted its own written litigation hold (DX-17; JX-22; July 7 tr 105:15–108:10). The vice president of SKOUT's Cyber Intelligence Center testified that the GNY letter was the only preservation demand he had received since the commencement of this litigation (July 7 tr 108:8–10).

Further, Slack messages from December 16, 2021 through February 3, 2022 were not preserved, purportedly because SKOUT personnel did not believe they were relevant to the ransomware event (Khan Aff ¶32).

VII. Discovery Parameters

On March 25, 2022, GNY served its first set of document requests on SKOUT seeking, among other things, "All Documents and Communications Concerning the Cyberattack, including without limitation, (a) all internal Communications between and among SKOUT personnel and (b) all Communications between and among GNY and SKOUT personnel" (NYSCEF 196).

In May 2023, the parties agreed to a discovery time frame of July 1, 2020 – February 3, 2022 for issues related to the cyberattack incident, and October 1, 2017 – February 3, 2022 for the commercial aspects of the litigation (JX-37 [June 22, 2023 Email from S. Harrison to K. Spicer]). As explained below, the missing data from Zendesk, Elastic, and Slack were generated within the agreed-upon time frame.

On February 28, 2024, based on information revealed during depositions, GNY sent a discovery deficiency letter to SKOUT that requested, among other things, tickets listed in SKOUT's internal investigation on June 1, 2021; every ticket generated for the 500+ brute force alarms closed out by analysts as "failed attempts"; Slack channel communications between SKOUT relating to GNY from May and June 2021; and documentation showing the use cases implemented into SKOUT's SIEM to generate alarms in May to June 2021 (NYSCEF 197).

On April 25, 2024, SKOUT responded to GNY's discovery deficiency letter, stating that, with respect to the request seeking various tickets stored within SKOUT's internal platforms, including Zendesk, SKOUT would produce a spreadsheet containing information on all GNY

tickets. SKOUT further stated that it no longer had access to the Slack channel communications or to the use cases that were in place in May and June of 2021 (NYSCEF 198).

In August 2024, GNY moved for spoliation sanctions, arguing that SKOUT failed to preserve several of categories of the documents GNY requested (*id*. at 1). As noted above, by Decision and Order dated September 13, 2024, the Court denied the motion without prejudice due to disputed questions of fact to be resolved at an evidentiary hearing or at trial (NYSCEF 244). The Court, however, directed SKOUT to determine whether a database containing GNY-related alarms and alerts existed and, if so, to provide GNY with access to it. Thereafter, SKOUT identified an Elastic database containing alarms and alerts generated by its SIEM and routed to SOC analysts between May 19, 2021 and February 3, 2022 (JX-39 at 61).

VIII. Zendesk

In 2024, two years into this litigation, SKOUT manually deleted thousands of tickets from Zendesk, its customer service and ticketing platform where alarms, alerts, tickets, and related analysis were maintained (PX-42 at 8–11; July 7 tr 35:19–23, 72:11–18).

According to SKOUT, Zendesk informed SKOUT in February 2024 that it had exceeded its allowable storage limit for tickets (Russo Aff ¶¶14–16; July 7 tr 36:8–18). To free up storage space, SKOUT claims to have implemented a 15-month retention period for all clients, resulting in the deletion of tickets older than 15 months (Russo Aff ¶17; July 7 tr 53:5–24; DX-23). Those deletions included GNY-related tickets (July 7 tr 37:16–38:11). A senior SKOUT employee testified that SKOUT could have purchased an add-on from Zendesk that would have allowed it to retain the GNY tickets, but SKOUT did not implement that option (July 7 tr 54:3–8).

Instead, SKOUT exported GNY-related Zendesk data to a spreadsheet in CSV format prior to implementing the new 15-month Zendesk retention policy. However, the CSV export

occurred after SKOUT had manually deleted thousands of tickets (Khan Aff ¶¶ 21–23; Russo Aff ¶¶19–21; July 7 tr 43:2–12; DX-28 at 9-11). The spreadsheet file contains columns for ticket numbers, alarm types, timestamps, and closure codes (JX-45; July 7 tr 53:14–24, 58:3–20, 155:16–24). Moreover, GNY's expert testified that some of the underlying raw data from the tickets, including detailed analyst narrative notes, were not captured in the CSV export (Cole Aff ¶ 43; July 7 tr 149:8–22, 150:1–9).

IX. Elastic Database

Elastic is the repository that, according to SKOUT, stored historical alarm data generated by SKOUT's monitoring systems reflecting activity within GNY's network, including alarms related to the ransomware attack against GNY (July 7 tr 69:19–21, 72:19–21; JX-16).

In December 2024, after initially maintaining that SKOUT did not retain the actual alarms for GNY, SKOUT claimed to have found copies of GNY-related alarms and alerts stored in its Elastic database, which was made available to GNY for inspection (PX-1 ¶ 7; PX-74 at 24; JX-39 at 60-61; Kannan Aff ¶¶ 6–7). GNY's expert inspected the Elastic database on January 29 and February 13, 2025 to assess whether it was a duplicate of the data and information contained in the Zendesk database, as exported into the CSV file (Cole Aff ¶ 50).

GNY's expert (Dr. Cole) noted that the Elastic database contained a larger volume of data than what was contained in the CSV file extracted from Zendesk (Cole Aff ¶¶ 85-87). A SKOUT executive averred:

> Dr. Cole is correct that there is a larger volume of data in the Elastic database than the data contained in the Spreadsheet of Alarms and Alerts extracted from the Zendesk database for the same period of time. The Elastic database registers the same alarm and alert counts as the Zendesk spreadsheet. *However unlike in the Zendesk database, the Elastic database logs a distinct record for every ticket action, status change, closure, comment, and alert.* The separate documents containing changes make the Elastic database appear to have many more entries than Zendesk. Importantly, the subject of the alarm, type of alarm, the

> description of the alarm, the closure code and closure comment related to the alarm, are the same in the Spreadsheet of Alarms and Alerts and the Elastic database.

(NYSCEF 518, Khan Supp Aff ¶ 10 [emphasis added]).

GNY's expert further found that alarms from June 1, 2020 to May 18, 2021[5] were missing from the Elastic database (Cole Aff ¶¶ 51, 72; July 7 tr 132:16–25). That period overlaps with the timeframe for which the parties agreed discovery would be produced, and, according to GNY's expert, could offer information on potential initial reconnaissance and scanning activities that attackers typically conduct prior to launching a cyberattack (JX-37; July 7 tr 152:7–20). Accordingly, the missing data falls within the scope of the parties' agreed-upon discovery and bears on the claims asserted in this action.

SKOUT attributes the missing data to the "Log4j vulnerability," a security flaw outside of SKOUT's control that required remediation efforts that, according to SKOUT, resulted in the loss of certain historical alarm data (Kannan Aff ¶¶ 12–15; DX-13; JX-31 at 6–7). GNY's expert testified that he could not determine the specific impact of Log4j on SKOUT's systems without additional information (July 7 tr 139:6–20). The missing historical data leaves gaps in the record concerning the alarms generated by SKOUT's monitoring systems and the context necessary to evaluate how those alarms were analyzed by analysts (Cole Aff ¶¶ 51, 72–73; July 7 tr 132:16–25).

CONCLUSIONS OF LAW

The Court concludes that SKOUT failed to preserve certain relevant evidence after its duty to preserve arose. "A party seeking sanctions based on the spoliation of evidence must demonstrate: (1) that the party with control over the evidence had an obligation to preserve it at

[5] (except for alarms from February 22, 2021)

the time it was destroyed; (2) that the records were destroyed with a "culpable state of mind"; and finally, (3) that the destroyed evidence was relevant to the party's claim or defense such that the trier of fact could find that the evidence would support that claim or defense" (*VOOM HD Holdings LLC v EchoStar Satellite L.L.C.*, 93 AD3d 33, 45 [1st Dept 2012]). "Under New York law, spoliation sanctions are appropriate where a litigant, intentionally or negligently, disposes of crucial items of evidence ... before the adversary has an opportunity to inspect them" (*Jerrick Assoc., Inc. v Phoenix Owners Corp.*, 191 AD3d 472 [1st Dept 2021] [internal citation and quotation omitted]).

I. When SKOUT's Duty to Preserve Evidence Arose

The duty to preserve evidence is triggered when a party "reasonably anticipates litigation" (*VOOM*, 93 AD3d at 36). Reasonable anticipation of litigation arises "when a party is on notice of a credible probability that it will become involved in litigation" (*id*. at 43), which may be well before an adverse party threatens or initiates litigation (*see*, *e.g.*, *Mangual v New Life School*, 245 AD3d 647, 648 [1st Dept 2026] ["[t]he occurrence of the incident, which was serious enough to prompt the school to call the police to investigate, was sufficient to put defendants on notice of their obligation to preserve relevant evidence"]; *Fata v Heskel's Riverdale, LLC*, 223 AD3d 520, 521 [1st Dept 2024] ["The record establishes that although defendant knew of plaintiff's injuries and was therefore on notice that the video surveillance footage might be needed for future litigation, defendant nevertheless failed to take affirmative steps to preserve the footage, which was then automatically erased"]; *Maiorano v JPMorgan Chase & Co*., 124 AD3d 536, 536 [1st Dept 2015] ["[A]lthough this action was not commenced until more than a year after the accident, defendant was on notice on the day of the accident that the surveillance video footage might be needed for future litigation"]; *Jamindar v Uniondale*

Union Free School Dist., 90 AD3d 610, 611 [2d Dept 2011] ["A sanction for spoliation of evidence may be warranted even if the evidence was destroyed before the spoliator became a party to the subject lawsuit, provided it was on notice that the evidence might be needed for future litigation"]).

In certain circumstances, courts have cited a defendant's contemporaneous internal investigation of an incident as potentially suggestive of its understanding there was a reasonable prospect of litigation (*SM v Plainedge Union Free Sch. Dist.*, 162 AD3d 814, 818 [2d Dept 2018] ["Given the nature of the infant plaintiff's injuries and the immediate documentation and investigation into the cause of the accident by the defendant's employees, the defendant was clearly on notice of possible litigation"]; *Freienstein v Mandarin Oriental New York Hotel, LLC*, 44 Misc 3d 1220[A] [Sup Ct, NY County 2014] [defendant's notice to its insurer, photographs of the scene, incident report, payment for plaintiff's hospital treatment, and post-accident safety meeting demonstrated awareness of the credible probability of litigation and thus triggered a duty to preserve relevant physical evidence]; see also *Martin v Wetzel*, 2020 WL 6948982, at *2 [WD Pa Nov. 25, 2020]; *Phillips v Harmon*, 297 Ga 386, 397 [2015]).

Based on the evidence presented, the Court finds that SKOUT's duty to preserve evidence arose on June 2, 2021, after its internal investigation revealed troubling information that had been "mis-mapped" and sent to the wrong client and certainly by June 10, 2021 when it concluded (as discussed during an internal training session) that it had failed to provide certain "big red flag" alerts to GNY preceding the attack. Because SKOUT served as GNY's cybersecurity monitoring provider, it understood—or should have understood—that its monitoring and escalation practices would likely be scrutinized in the aftermath of a ransomware attack that disabled GNY's system and required emergency response measures. It had also

specifically stressed to GNY the importance of preserving evidence in the aftermath of a cyberattack.

Under these circumstances, a reasonable party in SKOUT's position should have anticipated the likelihood of litigation on June 2, 2021 (and certainly no later than June 10, 2021). The Court therefore finds that SKOUT's preservation duty arose at that time.

II. Culpable State of Mind

SKOUT's failures to preserve evidence constitute, at a minimum, gross negligence. "Failures which support a finding of gross negligence, when the duty to preserve electronic data has been triggered, include: (1) the failure to issue a written litigation hold, when appropriate; (2) the failure to identify all of the key players and to ensure that their electronic and other records are preserved; and (3) the failure to cease the deletion of e-mail" (*VOOM*, 93 AD3d at 45).

First, SKOUT failed to issue a litigation hold following the June 2021 ransomware attack. Testimony indicates that the first—and only—litigation hold SKOUT shared with its employees was GNY's December 16, 2021 demand letter (July 7 tr 108:8–10). By that time, potentially critical internal Slack communications from immediately before and after the ransomware attack already had been deleted. And even that December 2021 external communication was not supplemented by specific *internal* guidance as to specific steps employees were required to take to ensure that discovery information was maintained (*Arbor Realty Funding, LLC v Herrick, Feinstein LLP*, 140 AD3d 607, 609 [1st Dept 2016] [finding gross negligence where a party failed to institute a litigation hold for approximately two years after its preservation obligation arose]).

Second, SKOUT failed to ensure the preservation of certain relevant electronically stored information, including Zendesk ticket data and historical alarm data in Elastic. In particular, SKOUT manually deleted GNY-related Zendesk tickets after this litigation had already been commenced, and in the midst of discovery (*Clarke v Povella*, 210 AD3d 581, 582 [1st Dept 2022] [finding gross negligence where a party failed to take steps to preserve evidence after a demand was made, and offered vague explanations for its loss]). The Elastic database is also incomplete, as alarms generated from June 1, 2020 through May 18, 2021 were not preserved.

Third, as noted, Slack messages were not preserved because SKOUT did not suspend its routine deletion practices after its duty to preserve arose (*Einstein v 357 LLC*, 2009 N.Y. Slip Op. 32784[U] [N.Y. Sup Ct, New York County 2009] ["While the deletion of emails is not per se improper, particularly when such deletions occur in the ordinary course of business, the matter is quite different when litigation has commenced or is reasonably anticipated"]). Slack communications from May and June 2021 were automatically deleted pursuant to SKOUT's 30-day retention policy, and Zendesk tickets older than 15 months were manually deleted pursuant to a new retention policy implemented after February 2024, well after the commencement of this litigation. SKOUT analysts' narrative notes were not preserved in the exported CSV file.

Accordingly, the Court finds that SKOUT's failure to implement an effective litigation hold and to suspend deletion policies after its preservation duty arose constituted gross negligence.

III. Relevance and Prejudice

Where the evidence is determined to have been destroyed through gross negligence, the relevance of such evidence is presumed (*VOOM*, 93 AD3d at 46).

In addition to the presumption of relevance, the record independently supports a finding that the missing information was very likely relevant to this litigation. GNY's claims concern SKOUT's monitoring and response practices preceding the ransomware attack, including alleged failures to properly identify and escalate malicious activity and the improper closure of brute-force alarms. The missing materials include Zendesk ticket data, including analyst narrative notes; historical alarm data from Elastic; and Slack communications among SKOUT analysts. Such evidence could shed light on the volume of alarms generated and the manner in which SKOUT analysts reviewed and closed those alarms, as well as SKOUT's internal discussions concerning suspicious activity.

Expert testimony further indicates that historical alarm data in Elastic may reveal patterns of reconnaissance or suspicious activity preceding a cyberattack. Although SKOUT produced a CSV export of certain Zendesk ticket data, testimony established that the exported format did not capture all contextual information reflected in the native system, including analyst narrative notes which might be important in determining whether and to what extent the attack could have been avoided. Slack communications likewise could have reflected contemporaneous internal discussions among SKOUT personnel regarding alerts, escalation decisions, and suspicious activity within GNY's network.

Accordingly, the Court finds that the missing evidence is relevant and that GNY was prejudiced by its loss.

IV. Appropriate Sanction

The Court concludes that an adverse inference and an award of reasonable attorneys' fees and costs constitute the appropriate sanction. New York "courts possess broad discretion to provide proportionate relief to a party deprived of lost or destroyed evidence, including the preclusion of proof favorable to the spoliator to restore balance to the litigation, requiring the spoliator to pay costs to the injured party associated with the development of replacement evidence, or employing an adverse inference instruction at the trial of the action" (*Pegasus Aviation I, Inc. v Varig Logistica S.A.*, 26 NY3d 543, 551 [2015]).

The imposition of an adverse inference is proportionate to the culpability established and prejudice shown. Although SKOUT's preservation failures were serious and constitute gross negligence, the Court declines to strike SKOUT's Answer. Striking a pleading is a drastic remedy generally reserved for cases involving willful or contumacious conduct or where the loss of evidence deprives the opposing party of the ability to prove its claim or defense (*Mylonas v Town of Brookhaven*, 305 AD2d 561, 563 [2d Dept 2003]; *Maiorano v JPMorgan Chase & Co.*, 2013 N.Y. Slip Op. 33787[U] [N.Y. Sup Ct, Bronx County 2013], affd, 124 AD3d 536 [1st Dept 2015]).

Here, there are at least some mitigating factors. With respect to Zendesk, SKOUT took steps to preserve data (albeit imperfectly) in CSV form, which did not include all of the information contained in the native system. Moreover, although certain Zendesk data, including analyst narrative notes, Elastic historical alarm data, and Slack communications are no longer available, other evidence concerning SKOUT's monitoring practices and its response to the ransomware incident remains in the record, including witness testimony and other documentary evidence produced during discovery.

Under these circumstances, the Court finds that the prejudice to GNY can be adequately addressed through a proportionate evidentiary sanction rather than the drastic remedy of striking SKOUT's Answer (*VOOM*, 93 AD3d at 47 [affirming an adverse inference, rather than striking the answer, where destroyed emails were relevant but the opposing party retained other evidence to prove its case]). An award of attorneys' fees and costs is likewise warranted because SKOUT's preservation failures necessitated extensive motion practice and an evidentiary hearing to address the loss of evidence and its consequences.

* * * *

Accordingly, it is

ORDERED that GNY's motion for spoliation sanctions (Mot. Seq. 10) is **GRANTED** to the extent that:

(i) An adverse inference shall be drawn that the missing information from Slack, Elastic, and Zendesk would have been unfavorable to SKOUT; and

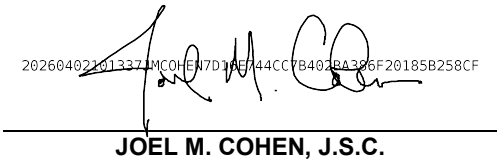
(ii) GNY is awarded reasonable attorneys' fees and costs incurred in connection with the present motion and the evidentiary hearing, the amount of which shall be determined upon submission of appropriate documentation; it is further

ORDERED that GNY submit its application for attorney's fees and costs with supporting documentation within fourteen (14) days of the date of this Order; Defendant shall have fourteen (14) days thereafter to file any objections. Plaintiff shall notify the Court via letter filing on NYSCEF and by email when the application is complete and whether it is opposed or unopposed; it is further

ORDERED that SKOUT's motion in limine to preclude GNY's expert report (Mot. Seq. 12) is **DENIED**; and it is further

ORDERED that SKOUT's motion in limine to preclude testimony and exhibits (Mot. Seq. 13) is **DENIED**.

This constitutes the Decision and Order of the Court.



4/2/2026
DATE

JOEL M. COHEN, J.S.C.

CHECK ONE:		**CASE DISPOSED**		[X]	**NON-FINAL DISPOSITION**		
	[X]	**GRANTED**	[ ] **DENIED**	[ ]	**GRANTED IN PART**	[ ]	**OTHER**
APPLICATION:	[ ]	**SETTLE ORDER**		[ ]	**SUBMIT ORDER**		
CHECK IF APPROPRIATE:	[ ]	**INCLUDES TRANSFER/REASSIGN**		[ ]	**FIDUCIARY APPOINTMENT**	[ ]	**REFERENCE**