UNITED STATES DISTRICT COURT SOUTHERN DISTRICT OF NEW YORK

Albert Rojas,
Plaintiff,

v.

340B Technologies Inc. d/b/a Nuvem Health LLC,
Defendant.

Case No. 1:25-cv-04684 (JGK)(JW)

Declaration of Albert Rojas Under 28 U.S.C. § 1746

This declaration is submitted in opposition to Nuvem's pretextual assertion of termination for attendance and in support of Defendant's retaliation defense

I, Albert Rojas, declare as follows:

1. On October 17, 2023, two days before my October 19 objection, I circulated an internal email regarding Solar Winds access requirements (Exhibit A). In that message, I explicitly warned management that Solar Winds required a database user with "master key" access to system tables — equivalent to being a Server Admin or Active Directory Admin — and cautioned that this level of access posed unacceptable risk to Plaintiff's systems containing PII data.

2. On October 19, 2023, I was instructed to provision a sysadmin-level "master key" account for a third-party vendor's access to Plaintiff's production servers containing PII (Exhibit C). At 9:43 a.m., I filed a breach notification with the U.S. Department of Health & Human Services, Office for Civil Rights (OCR), alerting regulators to this directive (Exhibit B). At 9:56 a.m., I informed Plaintiff's VP of R&D that I had filed the HHS report, writing: *"I know its my 4th day, but please we cannot provision … a sysadmin account for Madeira access … I submitted a breach notice with hhs.gov so that we protect Nuvem."* (Exhibit C).

3. That evening, at **8:59 p.m.**, I emailed Plaintiff's Human Resources department requesting that my compliance objection be **formally archived** in my personnel file. HR responded the following morning at **8:32 a.m.**, confirming receipt and stating in writing: *"I will save this to your files."* (Exhibit D).

   Employer Knowledge – Direct Confirmation (Exhibit D)

   Earlier that same afternoon, **October 19, 2023**, my direct supervisor, **Luigi Squillante, Vice President of Research & Development**, sent an email explicitly acknowledging my federal disclosure:

"Please send me the confirmation you received from hhs.gov regarding the claim you submitted for our files."

This written request is **undisputed proof that Nuvem management possessed actual, contemporaneous knowledge** of my whistleblower report to the **U.S. Department of Health & Human Services, Office for Civil Rights (HHS OCR)**, on the very day it was filed. It further shows that the company treated the report as an internal record-keeping matter—**not** as misconduct or insubordination—thereby recognizing its legitimacy.

When viewed together, Luigi Squillante's acknowledgment and HR's follow-up email confirm that **multiple Nuvem executives, across both operational and compliance functions, were aware of and preserved my HHS OCR breach filing** before any alleged "attendance" or performance issues arose. These contemporaneous communications eliminate any plausible claim that the company was unaware of my protected disclosure.

This direct, written acknowledgment satisfies the **employer-knowledge element** of a retaliation claim under **18 U.S.C. § 1514A (Sarbanes–Oxley)** and **N.Y. Lab. Law § 740**, and it underscores a clear causal link between my protected activity and the adverse employment action that followed.

4. On October 20, 2023, I exchanged text messages with Nuvem IT administrator Joel Ignatovich (Exhibit E). During that exchange, I wrote: *"I'm the one that killed the Solar Winds provisioning yesterday. Nobody gets a sysadmin account on my watch."* Mr. Ignatovich replied: *"Lol that was my concern as well. We were on the same page for that."* This confirms that internal IT recognized and shared my concern about improper sysadmin provisioning.

5. On October 24, 2023 — my final morning of employment — I was logged in and corresponding with Nuvem's Vice President of IT Security, Compliance & Infrastructure, Michael Larke, and Vice President of R&D, Luigi Squillante (Exhibit F). At 8:18 a.m. I replied to Mr. Larke's company-wide "October is Security Awareness Month" communication with a professional, technical response referencing internal risk controls and insider-threat prevention. My email reflected continued engagement, punctual attendance, and alignment with Nuvem's stated cybersecurity objectives. There was no indication of misconduct or tardiness; to the contrary, the exchange demonstrates that I was performing my duties and contributing constructively to Nuvem's compliance culture.

6. Exhibit F therefore rebuts Plaintiff's post-hoc assertion that I was terminated for "attendance." The contemporaneous timestamp and professional tone show I was present, active, and performing core responsibilities that morning. Termination immediately following such correspondence underscores retaliatory motive and falls squarely within the protections of **18 U.S.C. § 1514A (Sarbanes–Oxley)** and **N.Y.**

Lab. Law § 740, which prohibit adverse action against an employee for making or participating in protected compliance disclosures.

7. Taken together, Exhibits A through F form a consistent, contemporaneous evidentiary chain: I identified the sysadmin/master-key risk (Ex. A); reported it to federal regulators (Ex. B); objected internally and was admonished (Ex. C); received HR acknowledgment (Ex. D); was corroborated by Plaintiff's IT administrator (Ex. E); and, days later, continued active and professional participation on the very morning of my termination (Ex. F). This sequence establishes protected activity, employer knowledge, and retaliatory discharge under federal and state whistleblower statutes.

I declare under penalty of perjury under the laws of the United States of America that the foregoing is true and correct.

Executed on October 26, 2025, at New York, NY.

Respectfully submitted,

/s/ Albert Rojas
Albert Rojas (Pro Se)
319 W. 18th Street, Apt 3F
New York, NY 10011
rojas.albert@gmail.com | (646) 866-1669

Exhibit Legend (Consolidated and Strengthened)

Exhibit A – October 17 2023 Solar Winds Email
Early written warning to management that Solar Winds required "master-key" access equivalent to **Server Admin/AD Admin**, establishing that Rojas raised compliance concerns before the dispute arose.

Exhibit B – HHS OCR Breach Filing Acknowledgment (Oct 19 2023 9:43 a.m.)
Official acknowledgment of HIPAA breach report identifying **Nuvem Health LLC** and describing the risk as "giving a third party administrative access… the master key to our healthcare customers." Demonstrates **protected disclosure** under federal whistleblower law.

Exhibit C – October 19 2023 Email (Madeira Access / Sysadmin Key Directive)
Email exchange with VP R&D **Luigi Squillante** showing Rojas refused to provision a sysadmin account and was admonished *"it is not your place to submit breach information."* Proves **employer knowledge and disfavor** toward protected activity.

Exhibit D – HR Acknowledgment (Oct 19–20 2023)
Includes VP Luigi Squillante's written request for the HHS.gov confirmation and HR's reply, "I will save this to your files."
Confirms executive-level knowledge and recordation of the protected disclosure.

Exhibit E – Text Messages with Joel Ignatovich (Oct 20 2023) (IT Administrator)
Confirms IT administrator shared Rojas's concern: *"Lol that was my concern as well."* Corroborates that Rojas's stance was compliance-aligned, not insubordinate.

Exhibit F – October 24 2023 Email (Security Awareness Month)
Morning-of-termination exchange showing continued professionalism and alignment with cybersecurity goals. Rebuts Nuvem's attendance-based pretext.

Exhibit G – Nuvem Console Screenshot / Supplemental Declaration
Identifies **Joel Ignatovich** as the sysadmin credential custodian. Provides technical confirmation of Exhibits E and F, completing the custody chain and demonstrating Nuvem's awareness of the master-key issue.

Evidentiary Chain

1. **Early Warning (Ex. A)** — Identified sysadmin/master-key risk.
2. **Protected Disclosure (Ex. B)** — Filed HHS OCR breach report.
3. **Contemporaneous Objection (Ex. C)** — Refused sysadmin provisioning.
4. **Employer Knowledge (Ex. D)** — HR acknowledged disclosure.
5. **Corroboration (Ex. E)** — IT administrator confirmed objection.
6. **Ongoing Professional Conduct (Ex. F)** — Active on day of termination.
7. **Technical Confirmation (Ex. G)** — Console screenshot verified custody chain.

Result: All seven events occurred within 72 hours, establishing clear causation between protected disclosure, employer knowledge, and retaliatory termination.