CHRISTOPHER FROST (SBN 200336)
chris@frostllp.com
KEVIN S. DICKER (SBN 179315)
kevin@frostllp.com
FROST LLP
10960 Wilshire Boulevard, Suite 2100
Los Angeles, California 90024
Telephone: (424) 254-0441
Facsimile: (424) 600-8504

Attorneys for Plaintiff and Proposed Class

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA, SAN FRANCISCO DIVISION

BEEYO LTD, individually and on behalf of all others similarly situated,

Plaintiff,

vs.

RAILWAY CORPORATION,

Defendant.

Case No. 3:26-cv-13191

CLASS ACTION COMPLAINT:

1. NEGLIGENCE
2. BREACH OF IMPLIED CONTRACT

JURY TRIAL DEMANDED

Plaintiff Beeyo Ltd ("Beeyo"), individually and on behalf of all others similarly situated, alleges the following against Defendant Railway Corporation ("Railway"), based on knowledge of its own circumstances and on information and belief, after investigation, as to other matters.

I. NATURE OF THE ACTION

This action arises from Railway's October 2026 security breach. Railway accepted customer credentials for use in its cloud hosting service but failed to protect them from unauthorized access and misuse. Beeyo seeks recovery of unauthorized third-party charges and reasonable incident-response costs for itself and similarly situated paying customers.

Beeyo paid for Railway's Pro service and entrusted it with a Google Cloud API key used by Beeyo's applications. During the breach, unauthorized use of that key generated approximately $2,770 in net charges. Beeyo also had to investigate the misuse, disable affected services, and replace credentials.

II. PARTIES

Beeyo Ltd is a company incorporated under the laws of Israel with its principal place of business in Kfar Chabbad, Israel. Beeyo paid for and operated the affected Railway workspace through its representative, Teddy Layani.

Railway Corporation is a Delaware corporation with its principal place of business at 535 Mission Street, Suite 1549, San Francisco, California 94105. Defendant's service agent is CSC – Lawyers Incorporating Service, which can be served at 2710 Gateway Oaks Drive, Sacramento, California 95833. Railway operates the cloud hosting platform at railway.com.[1]

III. JURISDICTION AND VENUE

Jurisdiction. This Court has subject-matter jurisdiction under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2)(B), (5)(B), and (6) (2024). Beeyo is a citizen of Israel, and Railway is a citizen of Delaware and California. On information and belief, the proposed Class has at least 100

[1] *Railway Corporation,* Bloomberg LEI, https://lei.bloomberg.com/leis/view/254900YYMQHF6X7ENY39 (last visited Oct. 28, 2026).

FROST

members and its aggregate claims exceed $5,000,000, exclusive of interest and costs, based on the incident's reported scope and the unauthorized charges and response costs described below.

This Court has general personal jurisdiction over Railway because Railway maintains its principal place of business in this District.

Venue is proper under 28 U.S.C. § 1391(b)(1) and (c)(2) (2024) because Railway resides in this District.

Divisional Assignment. Assignment to the San Francisco or Oakland Division is proper under Civil Local Rules 3-2(c)–(d) and 3-5(b). Railway is headquartered in San Francisco, where, on information and belief, it directed the security policies and decisions challenged here.

IV. FACTUAL ALLEGATIONS

A. Railway's Custody of Customer Credentials

Railway provides tools to build, deploy, and run applications. Its environment-variable feature stores configuration information and secrets and supplies them to customer applications during builds and operation. Storing credentials on Railway is an intended use of the service.[2]

Railway controls encryption and key management within its infrastructure. Before the incident, a Railway employee publicly confirmed that these controls applied across subscription plans and could not be configured by customers from their workloads.[3]

API keys authorize access to third-party services, including services that charge for usage. Railway knew or should have known that disclosure of those keys could permit unauthorized use billed to its customers. Protecting the keys therefore required effective restrictions on access and decryption.

B. The October 2026 Breach

Railway's preliminary report places the intrusion between October 20 and 22, 2026. The attacker progressed through internal systems, obtained credentials for Railway's continuous-

[2] *Using Variables,* Railway Docs, https://docs.railway.com/variables (last visited Oct. 28, 2026).

[3] brody, Comment to *Encryption at Rest Coverage for Hobby Services in EU West,* Railway Cent. Station, https://station.railway.com/questions/encryption-at-rest-coverage-for-hobby-se-05f05e27 (last visited Oct. 28, 2026).

integration environment, and used compromised credentials to decrypt a subset of stored customer environment variables.[4]

Railway estimated that approximately 100,000 workspaces, at most 1.85% of all workspaces, had potentially compromised variables. It could not identify precisely which variables were decrypted and sent broader warnings to customers it considered at increased risk.[5]

On October 21, Railway publicly urged customers to rotate stored credentials and inspect third-party logs for unusual activity. Railway also paused new builds and deployments while investigating.[6]

Railway acknowledged that, while deployments were paused, customers could not update their applications with replacement credentials.[7]

On information and belief, Railway failed to reasonably segregate internal privileges and restrict access to customer secrets and the means of decrypting them. Those failures allowed the attacker to turn access to internal systems into exposure of customer credentials.

Other customers have publicly reported unauthorized Gemini and Twilio charges and time spent replacing credentials following the incident.[8]

C. Beeyo's Experience and Injuries

Before the breach, Beeyo stored a Google Cloud API key in the GOOGLE_API_KEY environment variable across several production services on Railway. Its application used only Gemini 2.5 Flash and Gemini 2.5 Pro for text processing.

---

[4] Jacob Cooper & Angelo Saraceno, *Preliminary Report: Oct 21st Security Incident,* Railway Blog (Oct. 22, 2026), https://blog.railway.com/p/preliminary-report-october-security-incident.

[5] *Id.*

[6] Jacob Cooper, *Security Disclosure: Wednesday October 21st,* Railway Blog (Oct. 21, 2026), https://blog.railway.com/p/security-disclosure-wednesday-october-21st.

[7] *Railway Platform Outage,* Railway Status (Oct. 21, 2026, 22:10 UTC), https://status.railway.com/incident/QH8L8B3E.

[8] *Security Incident 21 Oct 2026: Unauthorized Charges and Request for Credit and Incident Details,* Railway Cent. Station, https://station.railway.com/feedback/security-incident-21-oct-2026-unauthori-eaff19e5 (last visited Oct. 28, 2026).

On October 24, 2026, Railway sent Beeyo a direct notice identifying its workspace as within a targeted, increased-risk group because the workspace contained a large number of environment variables.

On October 21 and 22, unauthorized use of the stored key generated approximately $2,770 in net charges to Beeyo's Google Cloud project, according to Beeyo's current estimate. The charges included models and image, video, and audio services that Beeyo's application did not use.

The timing and nature of the unauthorized usage, the key's storage on Railway, and Railway's notice support the inference that the key was taken in this breach. On information and belief, the attacker obtained and misused Beeyo's key through the compromised Railway systems.

Beeyo's representative disabled the affected generative-AI services, deleted the compromised key, created a restricted replacement key, and rotated related credentials. Beeyo diverted time and resources to those measures, investigating the charges, and seeking their reversal.

Beeyo seeks the unauthorized charges and its reasonable investigation, containment, and credential-replacement costs. Its Google Cloud credit request remains pending. Any recovery will account for credits or refunds received.

CLASS ACTION ALLEGATIONS

Beeyo brings this action under Federal Rule of Civil Procedure 23(a) and (b)(3) on behalf of the following Class:

> All persons and entities that paid Railway for services, whose environment-variable data stored on Railway were accessed without authorization during the October 20–22, 2026 security incident, and that incurred unauthorized third-party charges or expenses investigating, containing, or remediating the incident.

Excluded are Railway and its parents, subsidiaries, and affiliates; their officers and directors and their immediate families; and the judicial officers assigned to this action and their immediate families.

On information and belief, the Class includes at least 100 members, making joinder impracticable. Railway's customer and incident records, together with billing and response records, can identify Class members.

Common questions include whether Railway used reasonable safeguards for entrusted credentials; whether its access and decryption controls were deficient; whether it breached a duty or contractual undertaking; and the proper measure of resulting losses.

These questions predominate because they concern common security practices and the same intrusion into Railway's infrastructure. Railway's policies, access records, and forensic findings will supply common proof. Individual losses can be determined from provider billing and response records.

Beeyo's claims are typical: it paid Railway to host applications and hold credentials, its stored key was compromised, and it incurred unauthorized charges and response costs arising from the same security failures alleged for the Class.

Beeyo will fairly and adequately protect the Class. Its interests align with those of Class members, and it has retained counsel experienced in complex and class action litigation.

A class action is superior because individual claims are generally too small to justify separate litigation of the common security issues. Resolving those issues together will avoid duplicative proceedings and permit consistent treatment of claims arising from the same incident.

CAUSES OF ACTION

FIRST CAUSE OF ACTION
NEGLIGENCE

Beeyo incorporates paragraphs 1–31 and brings this claim on behalf of itself and the Class.

By undertaking custody and control of customer credentials, Railway owed Beeyo and the Class a duty to use reasonable care to protect them from unauthorized access, disclosure, and use. Railway controlled the internal systems and privileges that protected those credentials.

Railway breached that duty by failing to reasonably restrict and segregate access to customer secrets and the internal credentials enabling their decryption, as alleged above. The compromised internal privileges permitted access beyond the systems initially breached.

The theft and misuse of API keys for unauthorized third-party consumption was a foreseeable consequence of those failures. Reasonable safeguards would have prevented or limited the exposure and resulting losses.

Railway's negligence directly and proximately caused Beeyo and Class members to incur unauthorized charges or reasonable investigation, containment, and remediation costs, or both. They seek compensatory damages in amounts to be proved at trial.

SECOND CAUSE OF ACTION
BREACH OF IMPLIED CONTRACT

Beeyo incorporates paragraphs 1–31 and brings this claim on behalf of itself and the Class.

Through their conduct, Railway and its paying customers agreed that Railway would host their applications and receive, store, and use the credentials needed to operate them in exchange for fees. That undertaking included maintaining reasonable safeguards against unauthorized access to and use of the entrusted credentials.

Beeyo and Class members performed their obligations by paying Railway for services and providing the credentials needed for those services.

Railway breached its undertaking by failing to provide reasonable access and credential protections, permitting the unauthorized access described above.

Those breaches caused Beeyo and Class members to incur unauthorized third-party charges or reasonable incident-response costs, or both. Those losses were foreseeable when Railway accepted payment to host applications and hold their credentials. Beeyo and the Class seek compensatory damages in amounts to be proved at trial.

PRAYER FOR RELIEF

Beeyo requests that the Court:

A. Certify the Class under Rule 23(b)(3), appoint Beeyo as Class representative, and appoint its counsel as Class counsel;

B. Award compensatory damages in amounts proved at trial, accounting for applicable credits and refunds and without duplicative recovery;

C. Award prejudgment and postjudgment interest and taxable costs as permitted by law;

D. Award reasonable attorneys' fees and expenses from any common fund created for the Class, as permitted by law; and

E. Grant such other relief as the Court deems proper.

DEMAND FOR JURY TRIAL

Beeyo demands a jury trial on all issues so triable.

DATED: November 4, 2026

FROST LLP

By: 

CHRISTOPHER FROST
KEVIN S. DICKER

HALL ATTORNEYS, P.C.
Nicholas Hall (*Pro Hac Vice forthcoming*)
Attorneys for BEEYO LTD.