

FOR IMMEDIATE RELEASE

Hall Attorneys and Co-Counsel File Class Action Over Ledger / Global-e Data Incident and Targeted Cryptocurrency Theft

S.D.N.Y. complaint alleges a December 2025 Global-e cloud-system compromise exposed Ledger customer and order information later used in highly targeted impersonation and digital-asset theft schemes.

Filed complaint: www.hallattorneys.com/dockets/ledger

NEW YORK, New York - August 25, 2026 - Hall Attorneys, P.C. and co-counsel filed a putative class action on August 24, 2026 against Global-E Online Ltd., Global-e US Inc., Ledger SAS, and Does 1-10 in the U.S. District Court for the Southern District of New York. The matter is No. 1:26-cv-07222, ECF No. 1.

The complaint arises from a December 2025 compromise of a Global-e cloud system containing shopper order data for several brands, including Ledger. It alleges defendants failed to prevent, adequately disclose, and reasonably mitigate the foreseeable use of Ledger customer and order information in targeted cryptocurrency-theft schemes.

According to the complaint, Global-e operated the integrated checkout and merchant-of-record platform used for Ledger.com transactions in the United States and Canada. The complaint alleges that identifying a person as a Ledger customer can reveal a security-sensitive relationship and help criminals construct convincing calls, emails, websites, or support interactions aimed at obtaining wallet recovery information.

Shopper-order data, not a direct wallet compromise

The complaint states that Ledger hardware, software, private keys, recovery phrases, and blockchain balances were not compromised in the Global-e incident. It likewise notes statements that payment-card data and account credentials were not accessed. The lawsuit instead focuses on the alleged use of names, contact details, shipping information, purchase history, device details, and related customer information to identify and authenticate likely cryptocurrency holders.

Targeted impersonation and alleged losses

The complaint alleges organized actors targeted Ledger customers in 2026 with layered impersonation campaigns. It says attackers used current customer-specific facts and caused genuine Ledger communications to arrive during the attacks, increasing the apparent credibility of fraudulent calls and interfaces.

Without identifying affected customers in this release, the complaint alleges two completed digital-asset thefts valued at more than US \$2.6 million in total at filing-time values. It does not allege defendants participated in those criminal thefts or that the current record conclusively identifies the source of every fact used by the attackers.

Proposed classes, claims, and requested relief

The complaint proposes a North American Ledger/Global-e Data Breach Class, a Targeted Impersonation Subclass, and a Digital-Asset Loss Subclass. It asserts negligence, breach of implied contract, breach of confidence, restitution and unjust enrichment, and declaratory and injunctive relief.

Requested relief includes damages and restitution; complete individualized notice; independent security assessments; merchant-tenant segmentation; least-privilege access; logging and anomaly detection; data minimization and secure deletion; victim-assistance measures; and safeguards intended to prevent misuse of genuine Ledger support and Ledger Recover communications.

Information for Ledger customers

U.S. and Canadian Ledger customers may want to contact the firm if they made a Ledger.com purchase processed through Global-e, received incident-related notice, or experienced a targeted Ledger-, Global-e-, Ledger Recover-, CoinCover-, police-, or security-themed contact using current customer, order, device, service, address, or support details.

In an initial message, provide your state or province, general purchase timeframe, device or service involved, and a short description of any targeted contact, attempted theft, or loss. Do not send wallet recovery information, private keys, PINs, passwords, authentication codes, or unredacted identity or financial records.

PRESERVE RELEVANT RECORDS

Ledger and Global-e order records, notices, support and verification emails, call logs, voicemails, suspicious messages, domains, screenshots, transaction exports, transaction hashes, reports, and loss records may be important.

Important security warning: Never share a recovery phrase, private key, PIN, password, or authentication code. Hall Attorneys will not ask for wallet secrets or direct you to move digital assets.

Important documents

Case overview: hallattorneys.com/ledger-data-breach

Filed complaint: hallattorneys.com/dockets/ledger

MEDIA AND CASE INQUIRIES
Nicholas Hall | Hall Attorneys, P.C.
nhall@hallattorneys.com | +1 713 428 8967
www.hallattorneys.com

Hall Attorneys is a Texas-based law firm focused on complex litigation. This release summarizes allegations in a filed complaint. The defendants have not yet had an opportunity to respond, no findings have been made, and no class has been certified. Sending information does not create an attorney-client relationship.

###