Z E R O T R A C E L A B S

A T T A C K C A S E S T U D Y

Ledger-Global-e Customer Data Breach & Phishing Campaign: Supply Chain Data Exposure at Scale

Third-party e-commerce partner compromise exposes Ledger customers to targeted phishing, reprising the company's worst operational nightmare.

Attack Snapshot

victim	Ledger SAS and its retail customer base
date	2026-02
loss	Undisclosed (PII of an undetermined number of customers compromised; downstream financial losses from phishing unquantified)
attack Type	Third-party data breach leading to targeted phishing campaigns
chain	N/A — off-chain, supply chain data breach
attribution	Unattributed; threat actors leveraged compromised Global-e data

Executive Summary

In February 2026, Ledger disclosed that its e-commerce payment processing partner, Global-e, suffered a data breach that exposed customer PII including full names, shipping addresses, email addresses, phone numbers, and order details for Ledger hardware wallet purchasers. Threat actors weaponized this dataset to launch highly targeted phishing campaigns against Ledger customers, leveraging order-specific details to craft convincing lures designed to extract seed phrases and wallet credentials. The incident is operationally analogous to Ledger's 2020 Shopify-linked breach and underscores a persistent, structural vulnerability in hardware wallet distribution: the e-commerce supply chain itself becomes an attack surface. The downstream financial impact remains undisclosed, but the breach materially increased the physical and digital threat profile for every exposed customer.

What Happened

Ledger, the France-based manufacturer of market-leading hardware wallets, confirmed in February 2026 that customer data had been compromised through a breach at Global-e, the third-party platform handling payment processing and cross-border e-commerce logistics for Ledger's online store. The breach exposed a dataset rich enough to be immediately operationalized: full names, physical shipping addresses, email addresses, phone numbers, and granular order details including product models and purchase dates. The exact timeline of the Global-e compromise remains unclear, but Ledger's disclosure indicated the company was notified by Global-e after anomalous data exfiltration was detected in the partner's infrastructure.

Within days of the breach becoming known — and likely before public disclosure — affected customers began reporting phishing emails and SMS messages that referenced their specific Ledger orders. The lures were sophisticated: they impersonated Ledger support communications, referenced correct order numbers and device models, and directed victims to credential-harvesting domains mimicking Ledger's recovery verification interface. Some campaigns included physical mail sent to exposed shipping addresses, instructing recipients to 'verify' their devices by scanning a QR code linked to a malicious site requesting seed phrase entry. The physical-mail vector is particularly insidious because it exploits the implicit trust consumers place in postal correspondence, especially when it references a real purchase.

This incident is structurally identical to the 2020 Ledger data breach, which was facilitated through a vulnerability in Shopify's third-party data access. In that case, approximately 272,000 customer records — including physical addresses — were leaked, leading to years of phishing campaigns and even reported physical threats against high-value targets. The 2026 Global-e breach demonstrates that despite Ledger's stated remediation efforts after 2020, the fundamental architectural risk persists: any third-party vendor with access to customer fulfillment data represents an unmitigated lateral attack surface.

Global-e, a publicly traded company (NASDAQ: GLBE) specializing in direct-to-consumer cross-border e-commerce, has not disclosed the full scope of the breach or the technical vector. It is unknown whether the compromise resulted from a vulnerability in Global-e's platform, a compromised employee account, or an API-level data exposure. Ledger stated it was working with Global-e and relevant data protection authorities, but declined to quantify the number of affected customers.

The downstream consequences extend beyond digital phishing. Exposed physical addresses create a durable threat: hardware wallet owners are now identifiable as cryptocurrency holders at specific residential locations. This data does not expire and cannot be rotated like a password. For affected customers, the breach creates a permanent elevation in physical security risk, including the possibility of targeted robbery or coercion attacks (the so-called '$5 wrench attack'). The reputational cost to Ledger is compounded by the recurrence — a second major supply-chain data breach erodes the trust proposition that is core to a hardware security company's value.

Ledger reiterated that its hardware and firmware were not compromised and that no legitimate Ledger communication would ever request a recovery phrase. The company

offered affected customers identity monitoring services and published updated phishing awareness guidance. However, these are reactive measures. The structural question — whether a hardware wallet manufacturer can safely outsource e-commerce fulfillment to third parties without creating existential data risk for its customers — remains unresolved.

Kill Chain

1. **Third-party compromise**
   Threat actors breached Global-e's infrastructure, gaining access to Ledger's customer fulfillment dataset including names, addresses, emails, phone numbers, and order details. The technical vector at Global-e has not been publicly disclosed.
2. **Data exfiltration and enrichment**
   Customer PII and order metadata were exfiltrated from Global-e systems. The dataset was likely enriched or cross-referenced with prior Ledger breach data (2020) to build comprehensive victim profiles, including device models owned and purchase history.
3. **Weaponized phishing campaign deployment**
   Attackers launched multi-channel phishing campaigns (email, SMS, physical mail) using order-specific details to impersonate Ledger. Lures directed victims to cloned Ledger interfaces designed to harvest 24-word recovery seed phrases and, in some cases, Ledger Live credentials.
4. **Wallet compromise and fund extraction**
   Victims who entered seed phrases on phishing sites had their wallets immediately drained. Attackers imported the seed into their own wallet software and transferred assets across multiple chains. Some reports indicate funds were routed through mixers and cross-chain bridges within minutes of seed capture.

Where Users Failed Themselves

— Entered 24-word recovery seed phrases into websites — the single action Ledger explicitly and repeatedly warns against in all official communications and device setup flows.

— Trusted email and physical mail communications at face value because they contained accurate order details, without independently verifying through Ledger's official channels (ledger.com directly, not via links in the communication).

— Used their primary personal email and phone number for hardware wallet purchases, creating a direct link between their identity, physical location, and cryptocurrency holdings.

— Failed to recognize that Ledger will never request seed phrase verification, firmware re-authentication via QR code, or account validation through email or postal mail.

— Did not use PO boxes, forwarding addresses, or pseudonymous shipping for hardware wallet deliveries, despite the precedent set by the 2020 breach demonstrating the risk of address exposure.

Prevention Checklist

FOR INDIVIDUAL USERS

☐ Never enter your seed phrase anywhere except the physical Ledger device itself during a recovery process you initiated. No website, app, or support agent will ever legitimately request it.

☐ Use a dedicated, compartmentalized email address for hardware wallet purchases — not your primary email. Consider a privacy-focused provider with no identity linkage.

☐ Ship hardware wallets to a PO box, commercial mail receiving agency, or forwarding address. Never link your residential address to a cryptocurrency hardware purchase.

☐ Treat any communication referencing your Ledger order — email, SMS, or physical mail — as potentially adversarial. Verify independently via ledger.com typed directly into your browser.

☐ Enable all available account security on Ledger Live (strong unique password, 2FA) and monitor for unauthorized login attempts.

FOR PROTOCOLS & PROJECTS

☐ Minimize the data shared with third-party e-commerce and fulfillment partners to the absolute operational minimum. Implement tokenization of customer PII at rest in partner systems.

☐ Require contractual and auditable security standards (SOC 2 Type II, penetration testing cadence, breach notification SLAs) from all third-party vendors with access to customer data.

☐ Implement proactive breach monitoring: deploy canary records in partner databases and monitor for their appearance on dark web markets.

☐ Architect e-commerce fulfillment so that no single third party holds the complete customer record (name + address + email + order details). Compartmentalize data across systems.

☐ Establish a rapid-response customer notification pipeline that can reach affected users faster than attackers can operationalize stolen data.

FOR THE ECOSYSTEM

☐ Hardware wallet manufacturers should offer an anonymous purchase option (cryptocurrency payment, no-KYC, pseudonymous shipping) as a first-class product feature, not an afterthought.

☐ Industry bodies should establish a data breach disclosure standard specific to cryptocurrency-adjacent companies, with mandatory notification timelines shorter than GDPR's 72 hours given the immediacy of downstream financial risk.

☐ E-commerce platform providers serving the crypto industry should be subject to heightened security certifications and independent audits, reflecting the elevated threat profile of their customer datasets.

Key Takeaway

Your hardware wallet's firmware can be impeccable — but if the company that sold it to you leaks your name, address, and order details through a third-party vendor, you become a target at home and online. Supply chain data security is not a peripheral concern; for hardware wallet users, it is the attack surface.

S O U R C E S

— Ledger official security incident disclosure (February 2026)
— Global-e (GLBE) data breach notification filings
— Ledger 2020 data breach post-mortem and Shopify third-party access incident (historical precedent)
— Community-reported phishing samples and physical mail lures (Reddit r/ledgerwallet, X/Twitter)
— ZeroTraceLabs internal threat intelligence on post-breach phishing campaign infrastructure