UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

JULIE COCHRANE and ANDREY TIURPENKO, individually and on behalf of all others similarly situated, Plaintiffs, v. **GLOBAL-E ONLINE LTD., GLOBAL-E US INC., LEDGER SAS, and DOES 1-10,** Defendants.	**Case No. _____** **CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

Plaintiffs Julie Cochrane and Andrey Tiurpenko (collectively, "Plaintiffs"), individually and on behalf of all others similarly situated, allege the following against Defendants Global-E Online Ltd., Global-e US Inc., Ledger SAS, and Does 1–10 (collectively, "Defendants") upon personal knowledge as to themselves and their own acts, and upon information and belief as to all other matters after an investigation by counsel that is continuing:

NATURE OF THE ACTION

1. This putative class action arises from a December 2025 compromise of a Global-e cloud system that contained shopper order data for several brands, including Ledger, and from Defendants' alleged failure to prevent, adequately disclose, and reasonably mitigate the foreseeable use of Ledger customer and order information in highly targeted cryptocurrency-theft schemes.

2. Global-e is not a peripheral payment vendor. It operates an integrated, white-label, cross-border e-commerce platform, acts as merchant of record, collects and processes shopper and order information throughout the transaction lifecycle, and supports thousands of merchants. Ledger

placed Global-e in the center of the Ledger.com checkout relationship for customers in the United States, Canada, and other markets.

3. Global-E Online Ltd. publicly disclosed that, in December 2025, it identified unauthorized access to one of its cloud systems and that names and contact information were impacted. Ledger separately disclosed that the system contained shopper order data from several brands and that some affected records pertained to Ledger.com purchases processed through Global-e as merchant of record.

4. The incident therefore appears to have a platform-level hub-and-spoke structure: Global-e was the common e-commerce and data-processing hub, while Ledger and other merchants were individual brand spokes whose shoppers' order records resided in the affected environment. The complete set of affected merchant spokes, shoppers, fields, and records remains exclusively within Defendants' possession.

5. The Ledger spoke carried an unusually dangerous risk. A record identifying a person as the purchaser of a Ledger hardware wallet or Ledger-related service does more than identify an ordinary retail preference. It identifies a person as a likely holder of digital assets and supplies the foundation for targeted social engineering designed to obtain a recovery phrase and drain an irreversible cryptocurrency wallet.

6. Defendants have stated that payment-card data, account credentials, private keys, recovery phrases, and blockchain balances were not accessed in the Global-e incident. Plaintiffs do not allege otherwise. The core allegation is that identity, contact, shipping, order, device, product, price, purchase-history, or related customer information can identify and authenticate a high-value target even without directly exposing the target's recovery phrase.

7. The risk materialized. In 2026, organized actors targeted Ledger customers with layered impersonation schemes that used preexisting customer-specific or device-specific knowledge and genuine Ledger communications to create credibility. The attackers then routed victims to fraudulent websites designed to obtain enough recovery information to reconstruct their wallets.

8. Plaintiff Cochrane lost cryptocurrency valued at approximately CAD $909,149.73 at the time of the transfers after callers who knew of her Ledger Recover relationship invoked CoinCover, caused a genuine Ledger Recover email to arrive during the call, and directed her to a newly registered fraudulent recovery website.

9. Plaintiff Tiurpenko lost approximately 30.01 Bitcoin, valued at about US $1.99 million at the time of transfer, after a staged law-enforcement-to-Ledger impersonation scheme in which the actors knew his exact Ledger device, recent purchase timing, and an existing battery problem, and caused a genuine Ledger support-verification email to arrive contemporaneously with the attack.

10. Both Plaintiffs made relevant Ledger.com purchases after the July 2020 Ledger e-commerce breach. Cochrane's attackers allegedly knew of a 2025 Ledger Recover relationship that did not exist at the time of the 2020 breach. Tiurpenko purchased his Ledger device in September 2025, and a check of the Have I Been Pwned service did not identify his email address in the 2020 Ledger breach corpus.

11. A threat-actor advertisement published after the incident purports to offer a "partial" Global-e/Ledger corpus and claims tens of thousands of Ledger-related records, including more than 30,000 U.S. records. The advertisement also references enrichment against older cryptocurrency-sector breach corpora and states that many users were not present in the older Ledger or Trezor data. The advertised totals are internally inconsistent, and Plaintiffs do not rely on the advertisement as proof of

an exact class count. It is nonetheless probative threat intelligence warranting discovery and preservation.

12. The available evidence thus suggests a second, criminal hub-and-spoke structure layered onto the first: a threat actor or data broker allegedly used the Global-e/Ledger corpus as one spoke in a broader enrichment hub that cross-referenced multiple cryptocurrency-related datasets. That enrichment model does not establish that Global-e was the source of every data element. It does support the reasonable inference that data from Defendants' systems could be combined with other data to identify, rank, and convincingly approach cryptocurrency holders.

13. Plaintiffs do not presently seek to represent shoppers of unrelated Global-e merchants without proper representatives and evidence showing that their records were affected. Plaintiffs plead the multi-merchant architecture because it bears directly on Defendants' security design, segmentation, notice obligations, the full scope of the incident, and the discovery needed to determine whether additional merchant-spoke classes should be added.

14. Plaintiffs seek relief for a North American Ledger/Global-e data-breach class, a targeted-impersonation subclass, and a digital-asset-loss subclass. They also seek individualized consequential damages for documented wallet losses, as well as declaratory, injunctive, restitutionary, and other relief available under applicable law.

15. Plaintiffs do not allege that Defendants participated in the criminal thefts or that the present record conclusively identifies the source of every item of information used by the attackers. Plaintiffs allege that Defendants' acts and omissions created or materially increased a foreseeable risk; that the risk manifested in targeted attacks; and that the decisive forensic, notification, support-log, and data-mapping evidence is controlled by Defendants and should be tested in discovery.

PARTIES

16. Plaintiff Julie Cochrane is a citizen of Canada domiciled in British Columbia. She is a Ledger customer, a Ledger Recover subscriber, and a consumer who made Ledger.com transactions after Global-e became Ledger's merchant-of-record partner.

17. On information and belief, Cochrane's pre-incident Ledger.com transaction and associated identity, contact, order, or service information were maintained within, transmitted through, accessible from, or linkable to the Global-e/Ledger customer-data environment implicated by the December 2025 incident. Defendants possess the records necessary to confirm the precise data lineage and affected fields.

18. Cochrane is a member of the proposed Classes because her Ledger customer relationship and genuine Ledger communication workflow were used in a targeted impersonation attack that caused completed digital-asset losses.

19. Plaintiff Andrey Tiurpenko is a citizen of Canada domiciled in British Columbia. He purchased a Ledger Flex device through Ledger.com in September 2025.

20. On information and belief, Tiurpenko's September 2025 Ledger.com transaction was processed by Global-e as merchant of record, and his identity, contact, shipping, device, order, price, purchase-date, or related data were maintained within, transmitted through, accessible from, or linkable to the affected Global-e/Ledger environment.

21. Tiurpenko is a member of the proposed Classes because attackers used exact device, purchase, and support-related knowledge, together with an authentic Ledger support-verification email, in a targeted impersonation scheme that caused the loss of approximately 30.01 Bitcoin.

22. Defendant Global-E Online Ltd. is an Israeli corporation with principal executive offices in Petah Tikva, Israel. It operates the Global-e enterprise platforms and publicly reports the December 2025 incident on a consolidated basis for itself and its wholly owned subsidiaries.

23. Global-E Online Ltd. describes its platform as a mission-critical, integrated, end-to-end e-commerce solution. It gathers extensive data across the lifecycle of an order, uses that data across its platforms, controls or participates in the security architecture of the affected cloud environment, and is responsible for incident investigation, disclosure, and remediation.

24. Defendant Global-e US Inc. is a Delaware corporation and a wholly owned significant subsidiary of Global-E Online Ltd. Its principal offices are at 200 West 41st Street, New York, New York 10018, within this District.

25. Global-e US Inc. is Global-E Online Ltd.'s U.S. agent for service of process. Ledger's sales terms identify Global-e US Inc. as the seller and merchant of record for customers located in the United States, Mexico, and Canada.

26. Global-e US Inc. contracted with consumers, collected and processed their personal and order information, accepted payment, appeared on transaction statements in connection with Ledger purchases, and participated in the integrated Global-e platform whose data environment was compromised.

27. Defendants Global-E Online Ltd. and Global-e US Inc. are referred to collectively as the "Global-e Defendants." They operated as an integrated enterprise with overlapping systems, policies, personnel, merchant relationships, incident response, data governance, and public disclosures. The precise allocation of responsibilities is within their exclusive knowledge.

28. Defendant Ledger SAS is a French société par actions simplifiée headquartered at 106 rue du Temple, 75003 Paris, France. Ledger manufactures and markets cryptocurrency hardware wallets and operates Ledger.com, Ledger customer support, Ledger-branded communications, and related services.

29. Ledger selected and integrated Global-e to facilitate Ledger.com transactions, continued to manufacture, package, handle, and support Ledger products, processed customer data as a data controller, administered consumer claims for Global-e, and remained responsible for Ledger's customer-support and post-sale communication systems.

30. Ledger knew that identifying information concerning its customers carries special risk because it identifies likely cryptocurrency holders. Ledger had direct experience with targeted phishing, physical threats, and wallet-drain schemes following its 2020 e-commerce data breach.

31. Defendants Does 1–10 are presently unknown persons or entities that owned, operated, secured, hosted, administered, supported, or controlled material portions of the affected systems, databases, support workflows, cloud infrastructure, or merchant integrations. Plaintiffs will amend after discovery identifies them.

32. At all relevant times, each Defendant acted through its agents, employees, contractors, affiliates, or co-venturers and within the course and scope of those relationships. Defendants' separate legal identities should not prevent relief where they jointly designed, operated, benefited from, or controlled the challenged systems and conduct.

JURISDICTION AND VENUE

33. This Court has original subject-matter jurisdiction under the Class Action Fairness Act of 2005 ("CAFA"), 28 U.S.C. § 1332(d).

34. The proposed Classes contain far more than 100 members. The threat-actor advertisement described above claims more than 30,000 U.S. Ledger-related records, while the exact affected population is ascertainable from Defendants' forensic, order, customer, and notification records.

35. The aggregate amount in controversy exceeds $5,000,000, exclusive of interest and costs. Plaintiffs alone allege completed digital-asset losses valued at more than US $2.6 million at the time of transfer, and the proposed Classes seek actual and consequential damages, mitigation costs, restitution, declaratory and injunctive relief, and other available remedies.

36. Minimal diversity exists under 28 U.S.C. § 1332(d)(2)(B). Plaintiffs are citizens or subjects of Canada, while Global-e US Inc. is a citizen of Delaware and New York for CAFA and general diversity purposes.

37. No mandatory CAFA exception applies. The proposed Classes include consumers distributed throughout the United States and Canada, and the challenged conduct involves foreign and domestic Defendants, a New York-based merchant-of-record entity, an international platform, and a multi-jurisdictional breach.

38. Plaintiffs have Article III standing because they allege concrete disclosure of personal and order information, completed targeted misuse, the loss of identifiable digital assets, mitigation time and expense, loss of use, privacy injury, and ongoing exposure to targeted attacks.

39. The injuries are fairly traceable to Defendants at the pleading stage. Plaintiffs allege a temporal and factual sequence involving post-2020 Ledger customer data, customer-specific knowledge, a December 2025 Global-e compromise, and the use of authentic Ledger communications

in 2026 attacks. Exact forensic allocation among Defendants and other contributing data sources is a merits question for discovery.

40. The requested relief is likely to redress Plaintiffs' injuries through compensation, restitution, security and data-minimization measures, improved incident disclosure, hardening of support-verification workflows, and other relief directed to the continuing risk.

41. This Court has general personal jurisdiction over Global-e US Inc. because it maintains its principal offices in this District and is at home here.

42. This Court has specific personal jurisdiction over Global-E Online Ltd. because it purposefully conducts and directs substantial U.S. business through its wholly owned New York subsidiary and U.S. agent, operates the integrated platform used by Global-e US Inc., stores and processes U.S. and Canadian shopper data, and publicly disclosed the incident giving rise to this action.

43. Global-E Online Ltd. has also purposefully availed itself of this forum by designating Global-e US Inc. at its New York principal offices as its U.S. agent for service, deeply integrating the parent's platform with the subsidiary's New York merchant-of-record operations, and deriving substantial revenue from transactions processed through those operations.

44. This Court has specific personal jurisdiction over Ledger because Ledger knowingly entered an ongoing merchant-of-record, sales-facilitation, data-processing, and customer-support relationship with a New York-based entity for U.S. and Canadian sales; integrated Global-e's white-label checkout into Ledger.com; directed consumer transaction data through that relationship; and the claims arise from that relationship and the resulting incident.

45. Ledger's published sales terms specifically identify Global-e US Inc. at its Manhattan address as the seller for U.S. and Canadian customers, while Ledger retains product, packaging,

logistics, support, after-sales, data-controller, and claims-administration responsibilities. Ledger could reasonably anticipate suit in New York over a breach arising from that arrangement.

46. Venue is proper under 28 U.S.C. § 1391(b)(1) because Global-e US Inc. resides in this District and all Defendants are residents of the United States or foreign entities for venue purposes.

47. Venue is independently proper under 28 U.S.C. § 1391(b)(2) because a substantial part of the events and omissions giving rise to the claims occurred in this District, including Global-e US Inc.'s merchant-of-record operations, contracting, data processing, governance, incident response, and New York-based participation in the integrated platform relationship.

48. Under 28 U.S.C. § 1391(c)(3), foreign Defendants may be sued in any judicial district, and their joinder is disregarded in determining venue as to other Defendants.

49. The Court may grant declaratory and further relief under 28 U.S.C. §§ 2201 and 2202 and has supplemental jurisdiction over all claims forming part of the same case or controversy under 28 U.S.C. § 1367.

FACTUAL ALLEGATIONS

A. Global-e Operates a Centralized Multi-Merchant Data Hub

50. Global-e markets itself as a leader in global e-commerce enablement and provides merchants with an integrated, end-to-end technology and services platform.

51. As of December 31, 2025, Global-e reported serving 1,547 merchants on its enterprise platforms and thousands of additional U.S.-based merchants through Shopify Managed Markets. Those figures describe Global-e's overall platform and do not establish that every merchant or shopper was involved in the December 2025 incident.

52. During 2025, Global-e enabled close to 30 million transactions across more than 30 origin countries and more than 200 destination markets. Global-e states that it gathers extensive data along the full order lifecycle—from the initial store visit through purchase, delivery, returns, fraud screening, customer support, and post-purchase activity.

53. Global-e functions in the background as a white-label component embedded into merchant websites. Shoppers may continue to perceive that they are dealing principally with the merchant brand even as Global-e becomes the seller, merchant of record, data controller, payment coordinator, fraud-screening operator, customer-support participant, or custodian of their order data.

54. Global-e publicly describes its accumulated transaction data as a vast, rich, and valuable data asset that permeates every layer of its platform and supports its "Smart Insights." It also operates customer-service portals, an AI-based chatbot connected to its systems and databases, and a manned contact center that can interact directly with shoppers or support merchant teams.

55. The platform architecture therefore creates concentration risk. A single access-control failure, cloud misconfiguration, compromised credential, or insufficiently segmented data environment can expose shopper records associated with multiple merchants and product verticals.

56. Global-e knew or should have known that multi-merchant data stores require rigorous tenant segregation, least-privilege access, logging, anomaly detection, data minimization, retention controls, encryption or tokenization, and incident-response capabilities capable of identifying each affected merchant and shopper record.

57. Global-e also knew or should have known that the sensitivity of a shopper record depends not only on the fields stored but also on the merchant and product revealed by the record. The

fact that a shopper bought an ordinary article of clothing presents a different foreseeable misuse profile than the fact that a shopper bought a hardware wallet designed to secure cryptocurrency.

58. Global-e assumed the role of merchant of record and seller for Plaintiffs' geographic market. That direct consumer relationship supplied Global-e with both the opportunity and the duty to design reasonable safeguards, limit retention, identify affected records, provide adequate notice, and prevent predictable downstream misuse.

B. Ledger Was a High-Risk Merchant Spoke

59. Ledger sells hardware devices used to secure access to Bitcoin and other digital assets. Ledger's marketing emphasizes that its devices protect the private keys that control those assets.

60. A Ledger order record therefore reveals a security-relevant affinity: the identified shopper likely owns cryptocurrency and has acquired a device associated with protecting it.

61. Names, email addresses, telephone numbers, home or shipping addresses, exact products, purchase dates, prices, order numbers, and service relationships can be used to select targets, establish credibility, tailor scripts, deliver physical mail, trigger genuine verification workflows, and induce victims to reveal recovery information.

62. The threat is amplified by the nature of self-custodied digital assets. Once a criminal obtains a recovery phrase and transfers assets, transactions generally cannot be reversed by a bank, payment processor, or centralized account provider.

63. Ledger had actual knowledge of these risks from the fallout of its 2020 e-commerce and marketing breach, after which Ledger customers received targeted phishing, threats, fraudulent devices and communications, and attempts to obtain recovery phrases.

64. Ledger nevertheless selected Global-e to act as the seller and merchant of record on Ledger.com and transmitted, caused to be transmitted, or permitted Global-e to collect customer identity and order information associated with Ledger purchases.

65. Ledger remained a data controller and retained responsibility for product manufacture, packaging, logistics, customer support, after-sales services, and administration of consumer claims on Global-e's behalf.

66. Reasonable care therefore required Ledger to evaluate Global-e's data architecture and retention practices, minimize sensitive merchant-affinity and order data, require reasonable security and segmentation, monitor known targeting patterns, provide prompt and direct warnings to affected customers, and harden Ledger's own communications against use as a credibility mechanism.

67. The allocation of duties among Ledger, Global-e, their affiliates, their cloud provider, and their support vendors is not available to consumers and is uniquely within Defendants' knowledge. Defendants cannot avoid accountability by shifting responsibility among entities that jointly operated the consumer relationship.

C. The December 2025 Global-e Platform Incident

68. In December 2025, Global-E Online Ltd. identified unauthorized access to one of its cloud systems. It later referred to the event as the "December 2025 Incident."

69. Global-e's 2025 annual report states that names and contact information were impacted and states that payment information, account credentials, and other sensitive personal data were not accessed.

70. Ledger's January 2026 incident notice provides additional context. Ledger states that the unauthorized party accessed a Global-e cloud-based information system containing shopper order

data from several brands and that some of the accessed data pertained to customers who purchased on Ledger.com using Global-e as merchant of record.

71. Ledger states that its hardware, software, private keys, recovery phrases, and blockchain balances were not compromised. Plaintiffs agree that the presently known incident involved e-commerce and order data rather than a direct compromise of wallet cryptography.

72. Defendants have not publicly disclosed the complete intrusion date range, initial access vector, affected cloud service, credential or vulnerability involved, duration of access, volume of exfiltration, identities of the other affected merchants, precise fields accessed for each shopper, number of affected shoppers, geographic breakdown, or whether the actor accessed historical order tables, support data, or linked datasets.

73. Defendants have also not provided Plaintiffs with a complete individualized accounting stating whether each Plaintiff's records were accessed, the precise fields involved, the systems containing those fields, the relevant retention periods, and the persons or entities with access.

74. On information and belief, Global-e retained independent forensic experts, contained portions of the incident, and notified some affected shoppers and regulators. The adequacy, timing, methodology, and completeness of those efforts remain unknown.

75. The fact that a multi-merchant cloud system was involved raises material questions concerning whether Global-e segregated merchant tenants, whether access to one merchant's records permitted access to others, whether data was stored in common tables or indexes, and whether incident response was capable of reconstructing record-level access.

76. Defendants' own public statements establish that the incident was not limited to Ledger. That makes the Global-e platform the common hub and the affected merchant datasets separate spokes.

77. Plaintiffs presently seek relief for the Ledger spoke because they purchased Ledger products and experienced Ledger-specific targeting. They reserve the right to amend to add additional merchant-spoke representatives and claims if discovery or investigation establishes a common compromise of other merchant populations.

D. Threat Intelligence Indicates a Ledger Corpus and Cross-Corpus Enrichment

78. On or about February 25, 2026, a user of a criminal breach forum advertised what the user described as a "partial" 2026 Ledger/Global-e dataset for the United States, United Kingdom, Australia, and several other countries.

79. The advertisement claimed "49,894" total lines plus additional countries and separately listed 30,907 U.S. records, 7,654 U.K. records, and 11,928 Australian records. Those regional subtotals equal 50,489 rather than 49,894.

80. Counsel has preserved a screenshot of the advertisement but has not purchased or independently authenticated the complete dataset. Plaintiffs therefore plead the advertisement as threat-intelligence evidence and a basis for discovery—not as conclusive proof of the exact affected count, fields, or provenance.

81. The advertisement described the records as including names, contact details, shipping addresses, and purchase history, while disclaiming recovery phrases, private keys, PINs, and payment-card details. The advertised description is broadly consistent with a shopper-order dataset but goes beyond Global-e's terse annual-report description of names and contact information.

82. The advertisement listed multiple source databases, including the purported Global-e/Ledger data and older cryptocurrency-sector customer, exchange, creditor, hardware-wallet, and transaction-related breach corpora.

83. The seller expressly acknowledged that some listed persons were returning Ledger customers present in older datasets but claimed that many users were unique and appeared in neither the 2020 Ledger data nor a Trezor corpus.

84. This presentation supports two reasonable and nonexclusive inferences: first, the seller obtained or possessed a Ledger-specific Global-e order corpus; second, the seller enriched or cross-referenced that corpus against other stolen or leaked data to improve targeting and valuation.

85. Cross-corpus enrichment is central to causation. A criminal campaign need not obtain every fact from one Defendant. Data disclosed by one source can be a substantial factor when it identifies the target as a Ledger customer, supplies a current address or device purchase, or corroborates other information that makes an impersonation credible.

86. Conversely, the presence of older data does not prove that the 2020 breach caused a 2026 attack. Post-2020 device purchases, service subscriptions, order dates, and support problems can function as temporal fingerprints distinguishing the new data from the older corpus.

87. Defendants' forensic evidence should reveal whether the fields and records described in the advertisement correspond to the affected Global-e tables; whether the threat actor possessed internal field names or ordering; and whether Plaintiffs' records were among the accessed or advertised population.

E. Ledger Knew Criminals Were Using Ledger Communications to Authenticate Calls

88. By at least May 13, 2026, Ledger had published a specific warning describing telephone impersonation campaigns targeting Ledger customers.

89. Ledger's warning described a tactic in which a scammer enters a victim's email address into a genuine Ledger support workflow, causing Ledger's own system to send an authentic confirmation email, and then immediately calls the victim while impersonating Ledger.

90. Ledger also warned that scammers invoked Ledger Recover and CoinCover and represented that urgent action was needed to protect the victim's assets.

91. The tactic exploits an intuitive but dangerous trust signal: the victim receives a genuine, contemporaneous Ledger communication and is told that the authentic sender domain proves the caller's legitimacy.

92. Ledger's publication of the warning establishes actual knowledge of the precise attack mechanism before Cochrane's May 28, 2026 loss and months before Tiurpenko's July 21, 2026 loss.

93. A website warning does not necessarily constitute reasonable mitigation for a known active campaign, particularly where Ledger and Global-e possessed the contact information needed to send direct warnings to the affected cohort and where the attackers exploited Ledger's own automated systems.

94. Reasonable mitigation could include authenticated initiation inside a logged-in support session; stronger friction before a third party can trigger an email to a customer; prominent contextual warnings at the top of every unsolicited verification message; flags when a support code is generated during a reported scam call; rate limits; anomaly detection; direct notification of affected customers; and correlation between threat reports, support logs, and Global-e incident records.

95. The reasonableness of any particular control is an expert and discovery question. Plaintiffs allege that Defendants did not implement a combination of controls sufficient to prevent the known workflow from functioning as an authentication device for organized theft.

96. Defendants also did not provide Plaintiffs with a complete, direct, individualized explanation that their identity and order information may have been exposed and that criminals were contemporaneously using genuine Ledger communications to authenticate unsolicited calls.

97. Defendants' public messaging emphasized that wallets, private keys, and recovery phrases were not directly compromised. Although technically accurate, that message risked understating the practical danger that stolen order and contact data could be used to persuade a customer to disclose the recovery information indirectly.

F. Plaintiff Cochrane's May 28, 2026 Attack and Loss

98. Cochrane is a long-time Ledger customer. She enrolled in Ledger Recover through Ledger.com in or about January 2025 and understood the service to include an additional recovery and security layer provided in connection with CoinCover.

99. Because the Ledger Recover relationship arose in 2025, knowledge of that relationship could not have come from the 2020 Ledger e-commerce corpus as it existed at the time of that breach.

100. On May 28, 2026, Cochrane received three calls in rapid succession. She answered the third call.

101. A male caller and a female caller, both speaking with British accents, represented that they were members of the cybersecurity team for Ledger Recover and stated that they were working with CoinCover.

102. Before Cochrane volunteered the information, the callers appeared to know that she was connected to Ledger Recover. They constructed an urgent narrative that her recovery arrangement or assets had been compromised and needed to be secured.

103. During the call, an authentic email from noreply@ledger.com arrived with the subject "Verify your email." It contained a six-digit code, referenced Ledger Recover, and displayed Ledger's branding.

104. The callers directed Cochrane to inspect the authentic ledger.com sender domain as proof that they were legitimate. The contemporaneous official communication materially reinforced the credibility of the call.

105. The email instructed the recipient to ignore the message if she had not made the request personally and warned never to share the 24 words of a recovery phrase or enter them anywhere other than a Ledger device. Cochrane did not knowingly disclose a complete recovery phrase to a caller.

106. When Cochrane refused to connect her Ledger device, the attackers immediately shifted to a prepared contingency path and directed her to ledgerrecoverhelp.com.

107. When Cochrane questioned the site, the callers told her to check it through Google Safe Browsing. She reports that the site displayed a safe or green result at that time.

108. The callers instructed Cochrane to enter only the first three or four letters of each recovery word, rather than the complete words. The instruction was designed to make her believe that she was not disclosing the full phrase.

109. Under the BIP-39 word list used for recovery phrases, the first four letters are sufficient to uniquely identify each word. The attackers could therefore reconstruct the complete phrase from the truncated entries.

110. The attackers also supplied replacement words, promised a replacement Ledger device within days, and promised a callback, further creating the appearance of an organized support process rather than an immediate theft.

111. Immediately after Cochrane entered the truncated recovery information, cryptocurrency left her control and began moving through recipient addresses.

112. Ledger transaction exports and public blockchain records document outgoing transfers on May 28, 2026 Pacific time, including approximately 6.01528818 BTC, 44.3937816580798 ETH, 133.611102997226 BNB, 407.868604103 SOL, 556.6855654675 LINK, and 1,887.106601 XRP.

113. At the operation-date values reflected in Cochrane's Ledger export, the transferred assets totaled approximately CAD $909,149.73. Plaintiffs reserve all rights concerning the legally appropriate valuation date, loss of use, prejudgment interest, and any recoverable post-theft appreciation.

114. The Bitcoin transaction sent approximately 6.01528818 BTC from Cochrane's account. After the network fee, approximately 6.01494378 BTC reached the first receiving address and was promptly split and forwarded through additional addresses.

115. The transaction records corroborate completed theft but do not, standing alone, identify the perpetrators or the source of the customer information used in the social engineering.

116. Cochrane reported the incident to law enforcement, including an FBI IC3 report on May 30, 2026, preserved her call records, emails, transaction exports, domain information, blockchain evidence, and later sent Ledger a detailed notice and preservation request.

117. Cochrane suffered the loss of digital assets, loss of use, substantial time and expense investigating and reporting the theft, emotional distress, anxiety, and a continuing risk of additional attacks because her immutable identity, contact, address, purchase, and cryptocurrency-affinity information remains in criminal hands.

G. Plaintiff Tiurpenko's July 21, 2026 Attack and Loss

118. Tiurpenko purchased an orange Ledger Flex device through Ledger.com in September 2025. The purchase occurred years after the 2020 Ledger breach.

119. A search of the Have I Been Pwned service did not identify Tiurpenko's email address as included in the 2020 Ledger breach corpus. Defendants' records and the underlying datasets will provide the definitive comparison.

120. On July 21, 2026, Tiurpenko received a call from a person impersonating a police officer. The caller stated that police had stopped a vehicle, found hundreds of stolen identities, and identified Tiurpenko as a potential victim.

121. The purported officer supplied a case number and told Tiurpenko that a cryptocurrency-company representative would contact him and that he should not speak with that person unless the person provided the same case number.

122. A subsequent caller provided the case number and transitioned Tiurpenko into a purported security or recovery process involving Ledger.

123. The attackers knew Tiurpenko owned a Ledger Flex with an orange case, knew when he had purchased it, and referenced a battery problem he had experienced. They used that information to establish credibility and appeared capable of discussing or helping with the device issue.

124. During the attack, an authentic Ledger-branded email from care@ledger.fr arrived with the subject "Here's your Ledger Support verification code." The email supplied a six-digit code and stated that a support session had been requested on Ledger's official website.

125. The email prominently warned not to share the code outside the chat window and instructed the recipient to ignore the email if he had not initiated a live-chat request.

126. The attackers' staged police contact, matching case number, exact post-2020 device and purchase knowledge, battery-issue knowledge, and contemporaneous authentic Ledger email combined to create a layered credibility structure.

127. The attackers directed Tiurpenko through fraudulent websites and purported recovery personnel. Tiurpenko ultimately entered recovery information into a fraudulent interface, after which the attackers obtained control of his wallet.

128. At approximately 18:48 UTC on July 21, 2026, approximately 30.00995812 BTC left Tiurpenko's account, with a recorded fee of approximately 0.00024552 BTC.

129. The Ledger transaction export valued the outgoing Bitcoin at approximately US $1,987,510.99 at the time of the transaction. Tiurpenko lost his life savings accumulated through approximately three decades in construction work.

130. Approximately one week later, another group again attempted a substantially similar police-themed approach. Tiurpenko recorded part of the call.

131. During the later call, the actors allegedly confirmed transaction details associated with his September 2025 Ledger.com purchase, further supporting the inference that the targeting relied on current order or customer information rather than only the 2020 corpus.

132. Tiurpenko preserved the authentic Ledger email, transaction export, recorded call segment, purchase information, device facts, and related materials.

133. Tiurpenko suffered the loss of digital assets, loss of use, investigation and reporting costs, severe emotional distress, anxiety, and ongoing risk of further targeted attacks.

H. Defendants' Alleged Security, Notice, and Mitigation Failures

134. Defendants had a duty to use reasonable care in collecting, transmitting, retaining, processing, accessing, securing, and disposing of consumer identity, contact, order, merchant-affinity, and support information.

135. That duty arose independently from the consumer contracts because Defendants created and controlled the risk, possessed specialized cybersecurity and e-commerce knowledge, invited consumers to entrust information to their systems, and knew that disclosure could expose cryptocurrency holders to targeted theft.

136. The Global-e Defendants breached their duties by one or more of the following acts and omissions, the precise combination of which will be established in discovery: failing to maintain reasonable cloud configuration and access controls; failing to enforce least privilege; failing to segregate merchant data; failing to adequately log and monitor access; failing to detect or contain exfiltration; retaining more data or for longer than reasonably necessary; failing to encrypt or tokenize sensitive order attributes where feasible; failing to test incident response; and failing to provide prompt, complete, individualized notice.

137. Ledger breached its duties by one or more of the following acts and omissions: failing to exercise reasonable oversight of Global-e; transmitting or permitting retention of unnecessary Ledger-affinity and order data; failing to require adequate segmentation and security; failing to correlate the Global-e incident with active Ledger-targeting campaigns; failing to directly warn affected customers; and failing to sufficiently harden support and Ledger Recover verification workflows known to be used by scammers.

138. Defendants also failed to clearly disclose the practical consequences of the incident. Statements that private keys, recovery phrases, and wallets were not directly compromised did not explain that order data could identify cryptocurrency holders and enable attackers to induce disclosure of those secrets.

139. Defendants failed to provide Plaintiffs a complete, field-level, record-specific explanation sufficient to determine what information was accessed, how long it had been retained, whether it had been exfiltrated, whether it appeared in the advertised corpus, and what concrete steps were necessary to mitigate the threat.

140. Defendants failed to offer remediation proportional to the risk, including monitoring for merchant-specific phishing, enhanced support-verification controls, direct threat notifications, assistance tracing targeted misuse, and reasonable compensation for documented losses caused by the foreseeable attacks.

141. On information and belief, Defendants continue to retain personal and order information in systems that remain attractive targets. Names, email addresses, telephone numbers, home addresses, purchase history, and merchant affiliation cannot all be changed and remain useful to criminals indefinitely.

142. Defendants' failures were a direct, proximate, foreseeable, and substantial factor in Plaintiffs' and Class members' injuries. The intentional conduct of criminal actors was itself the precise foreseeable risk created by exposing and inadequately mitigating cryptocurrency-holder information and does not categorically sever causation.

143. To the extent attackers combined Global-e/Ledger data with other datasets, each Defendant remains liable where its data, systems, or omissions materially contributed to target

selection, authentication, or completion of the theft. Multiple sufficient or concurrent causes do not eliminate responsibility at the pleading stage.

144. Plaintiffs anticipate that Defendants will assert comparative fault based on warnings in emails and Ledger's public guidance. Those arguments concern apportionment and the reasonableness of conduct under the totality of circumstances. They do not negate Defendants' antecedent duties, knowledge of the attack method, or the causal role of customer-specific information and authentic communications.

145. Plaintiffs further anticipate that Defendants may contend the attackers could have used the 2020 Ledger corpus. The post-2020 facts alleged here—including a 2025 Ledger Recover relationship, a September 2025 device purchase, exact device and battery information, and a negative HIBP result for Tiurpenko's email—make that alternative explanation a disputed factual issue rather than a basis for dismissal.

I. Plaintiffs' and Class Members' Injuries

146. Plaintiffs and Class members lost the benefit of their bargains because Defendants accepted their money and personal information without providing the reasonable security, confidentiality, data minimization, incident response, and notice that formed part of the transaction.

147. Plaintiffs and Class members suffered loss of privacy and confidentiality, diminution or loss of the value of their personal information, and exposure of information that identifies them as likely cryptocurrency holders.

148. Members of the Targeted Impersonation Subclass suffered completed or attempted phishing, vishing, smishing, physical-mail fraud, fraudulent support contacts, and other attacks that required time and money to investigate, report, and mitigate.

149. Members of the Digital-Asset Loss Subclass suffered completed theft of Bitcoin and other assets, loss of use, transaction fees, investigative expenses, and other consequential damages.

150. The valuation of stolen cryptocurrency presents individualized damages questions but does not defeat common liability issues. The Court may address those damages through subclasses, individual proceedings, a claims process, special masters, Rule 23(c)(4), or other case-management tools.

151. The affected data remains in criminal hands, may be combined with additional datasets, and can be reused in future campaigns. Plaintiffs and Class members therefore face a continuing, concrete risk of targeted attacks distinct from the generalized risk of ordinary spam.

152. Plaintiffs and Class members have incurred and will continue to incur reasonable mitigation costs, including time monitoring accounts and communications, changing contact information or security practices where possible, reporting incidents, obtaining forensic or legal assistance, and securing remaining assets.

153. Plaintiffs also suffer anxiety and loss of peace of mind arising from criminals' possession of their home addresses and knowledge that they likely hold digital assets.

THE OPERATIVE TERMS DO NOT DEFEAT THIS COURT'S AUTHORITY

154. Ledger's currently published Ledger-specific sales terms state that Global-e collaborates with Ledger as the merchant of record and that Global-e is the seller for purchases on Ledger's website.

155. Those Ledger-specific terms identify Global-e US Inc., a Delaware corporation with a Manhattan place of business, as the seller for customers located in the United States, Mexico, and Canada.

156. The Ledger-specific terms state that both Ledger and Global-e process and collect personal data, preserve mandatory consumer protections from the consumer's country of habitual residence when more favorable, and permit consumer disputes to be taken to a competent court.

157. The Ledger-specific terms do not contain a facial arbitration clause or class-action waiver and state that later changes do not affect orders already placed.

158. Global-e publishes a separate generic terms page that currently contains an arbitration clause directed to U.S. residents. Plaintiffs are Canadian residents, deny that the generic page governed or was conspicuously incorporated into their Ledger-specific purchase transactions, and deny any knowing and unambiguous assent to arbitrate these claims.

159. The historical terms, checkout screens, hyperlinks, version logs, clickstream evidence, receipts, and assent records applicable to each Plaintiff are controlled by Defendants and must be produced before any formation, incorporation, delegation, scope, or enforceability issue can be resolved.

160. To the extent Defendants invoke a liability limitation, consequential-damages exclusion, foreign-law clause, forum provision, arbitration term, or class waiver, Plaintiffs allege that it is inapplicable, was not reasonably communicated or assented to, does not reach independent tort and statutory duties, or is unenforceable to the extent prohibited by mandatory consumer law, public policy, gross negligence, or willful misconduct.

161. British Columbia's consumer-protection law renders pre-dispute consumer arbitration requirements and class-proceeding prohibitions void. Plaintiffs also reserve all rights under the mandatory consumer and privacy law of their habitual residence preserved by Defendants' own Ledger-specific terms.

162. Plaintiffs anticipate that additional U.S. representatives may be added. Any arbitration analysis for such persons must be conducted separately based on the exact transaction date, merchant-specific terms, checkout presentation, geographic clause, notice, and manifestation of assent.

163. No Defendant can manufacture retroactive assent through a later website revision. The Court must decide whether any agreement was formed before any purported arbitration rules or delegation provision can apply.

CLASS ACTION ALLEGATIONS

164. Plaintiffs bring this action under Federal Rules of Civil Procedure 23(a), 23(b)(2), 23(b)(3), and, as appropriate, 23(c)(4), individually and on behalf of the following proposed Classes, subject to amendment after discovery:

> **North American Ledger/Global-e Data Breach Class**: All natural persons residing in the United States or Canada whose personal, contact, shipping, order, purchase, device, product, price, or related Ledger customer information was accessed, acquired, exfiltrated, copied, or otherwise compromised in the December 2025 Global-e incident.
>
> **Targeted Impersonation Subclass**: All members of the North American Ledger/Global-e Data Breach Class who, after the incident, received an actual or attempted Ledger-, Ledger Recover-, CoinCover-, Global-e-, police-, or security-themed impersonation contact that used customer-specific, order-specific, device-specific, service-specific, address-specific, or genuine Ledger communication information reasonably traceable in whole or in material part to Defendants' systems or data.
>
> **Digital-Asset Loss Subclass**: All members of the Targeted Impersonation Subclass who suffered a completed unauthorized transfer or theft of cryptocurrency or other digital assets as a result of the targeted impersonation.

165. Plaintiffs are members of the proposed Classes. On information and belief, their Ledger.com order or customer information was within or linkable to the affected Global-e/Ledger

environment, they were subjected to targeted impersonation using current Ledger-specific information and genuine Ledger communications, and they suffered completed digital-asset losses.

166. Excluded from the Classes are Defendants and their parents, subsidiaries, affiliates, officers, directors, and employees; any entity in which a Defendant has a controlling interest; the judges and court personnel assigned to this case and their immediate families; and persons who validly request exclusion from a Rule 23(b)(3) class.

167. Plaintiffs reserve the right to amend, narrow, expand, or create U.S., state, provincial, Canadian, merchant-spoke, authenticated-communication, device-specific, support-workflow, statutory, or damages subclasses as the facts and law develop.

168. Plaintiffs do not presently define a class of shoppers associated with unrelated Global-e merchants. If discovery identifies other affected merchant spokes and appropriate representatives, Plaintiffs reserve the right to seek amendment or coordination consistent with Article III and Rule 23.

169. Numerosity is satisfied because joinder is impracticable. The threat-actor advertisement claims more than 30,000 U.S. Ledger records and tens of thousands of records across other markets, while Defendants acknowledge a multi-brand system. The exact count is ascertainable from Defendants' records.

170. Commonality is satisfied because the action presents common questions capable of generating common answers, including: whether and how the Global-e cloud system was compromised; what data was affected; whether merchant records were adequately segregated; whether Defendants used reasonable security and retention practices; whether Defendants provided adequate notice; whether Ledger's support and verification workflows were reasonably designed after actual notice of their misuse; and what classwide declaratory and injunctive relief is appropriate.

171. Additional common questions include whether Ledger exercised reasonable vendor oversight; whether customer and order data identifying cryptocurrency holders required enhanced safeguards; whether Defendants' conduct breached common contractual and confidence-based obligations; whether cross-corpus enrichment was foreseeable; and whether a common methodology can identify reasonably traceable misuse.

172. Typicality is satisfied because Plaintiffs' claims arise from the same incident, integrated merchant relationship, categories of data, alleged security and mitigation failures, and targeted misuse that give rise to the claims of the proposed Classes.

173. Plaintiffs' high-value losses do not make their claims atypical as to common liability. Those losses place them within the Digital-Asset Loss Subclass and can be adjudicated through subclass or individualized damages procedures after common issues are resolved.

174. Plaintiffs will fairly and adequately protect the Classes. They have no interests antagonistic to absent members, have preserved extensive evidence, and have retained counsel experienced in data-breach, privacy, cryptocurrency, and complex class litigation.

175. Plaintiffs' counsel include Milberg and Hall Attorneys. Counsel intend to commit the resources necessary to investigate, prosecute, finance, and try this action and to associate SDNY-admitted counsel as required.

176. Predominance is satisfied because common questions concerning the incident, platform architecture, duty, breach, notice, vendor oversight, support-workflow design, foreseeability, and classwide remedies predominate over individualized issues.

177. The possibility that some attacks used additional datasets does not defeat predominance. Common evidence can determine what data was exposed, whether particular post-2020 fields were

unique to the Global-e/Ledger environment, and whether Defendants' data was a substantial factor in defined categories of attacks.

178. Individual damages calculations do not defeat certification. Digital-asset quantities and transaction dates are objectively verifiable through transaction exports and public blockchains, and valuation can be determined using a common legal methodology followed by ministerial calculations.

179. A class action is superior because affected persons are geographically dispersed; many consumer-class damages are too small to litigate individually; the technical and forensic issues are expensive; Defendants possess the decisive evidence; and inconsistent individual rulings would be inefficient.

180. Even persons with substantial wallet losses benefit from common adjudication of the incident, duty, breach, warnings, support-system design, and causation framework while preserving individualized damages proceedings where necessary.

181. Certification under Rule 23(b)(2) is appropriate because Defendants have acted or refused to act on grounds generally applicable to the Classes and continue to retain data and operate common systems that create ongoing risks addressable through uniform declaratory and injunctive relief.

182. Certification under Rule 23(c)(4) is appropriate, in the alternative, for common issues concerning the scope of the breach, reasonableness of security, adequacy of notice, vendor oversight, Ledger support-workflow design, and classwide equitable relief even if individual causation or damages issues require later proceedings.

183. The Classes are ascertainable through objective criteria, including Global-e order and notification records, Ledger customer and support records, affected-table and forensic logs, email and telephone records, purchase dates, device information, and blockchain transactions.

184. Plaintiffs are unaware of any presently filed U.S. class action arising from this December 2025 Global-e/Ledger incident and the resulting 2026 targeted impersonation losses. Plaintiffs will advise the Court of any related proceeding identified before filing or during the litigation.

GOVERNING LAW, ALTERNATIVE PLEADING, AND TOLLING

185. Plaintiffs plead the common-law claims under New York law because substantial Global-e conduct occurred through its New York principal offices and merchant-of-record operations and because New York has a strong relationship to the challenged platform conduct.

186. The precise choice-of-law analysis depends on contracts, system responsibilities, data locations, merchant agreements, and conduct facts controlled by Defendants. Plaintiffs reserve the right to amend and subclass after discovery.

187. All claims are timely. The incident occurred in December 2025, was disclosed in January 2026, and Plaintiffs' targeted losses occurred in May and July 2026.

188. To the extent any limitation period is disputed, it is tolled by the discovery rule, fraudulent concealment, equitable tolling, Defendants' exclusive control of forensic facts, the continuing retention and misuse risk, and any applicable class-action tolling doctrine.

COUNT I
NEGLIGENCE
(Against All Defendants on Behalf of Plaintiffs and the Classes)

189. Plaintiffs incorporate the preceding allegations as though fully set forth here.

190. Defendants owed Plaintiffs and Class members duties of reasonable care arising from their collection, control, processing, transmission, integration, retention, security, and use of personal, contact, order, device, merchant-affinity, and support information.

191. The duties were independent of contract and arose from Defendants' creation and control of the risk, their special knowledge of the systems and threat environment, consumers' inability to protect data in Defendants' custody, and the foreseeable danger of identifying cryptocurrency holders to criminals.

192. The Global-e Defendants owed duties to design and maintain reasonable cloud security, tenant segregation, access controls, monitoring, data minimization, retention, incident response, forensic reconstruction, and notification practices.

193. Ledger owed duties to exercise reasonable vendor oversight, minimize and protect Ledger customer data, respond reasonably to the Global-e incident, provide adequate and direct warnings, and design or modify support and verification workflows after learning that criminals were using genuine Ledger communications to authenticate fraudulent calls.

194. Defendants breached those duties through the acts and omissions alleged above.

195. The targeted theft of cryptocurrency through social engineering was a foreseeable consequence of exposing information identifying persons as Ledger customers and failing to mitigate a known impersonation method.

196. The criminal actors' intentional conduct does not eliminate proximate cause because targeted impersonation and wallet theft were among the precise foreseeable harms that reasonable safeguards, warnings, and workflow controls were intended to prevent.

197. Defendants' conduct was a direct, proximate, concurrent, and substantial factor in Plaintiffs' and Class members' injuries even if criminals also used information from other sources.

198. Plaintiffs and Class members suffered the injuries alleged above, including disclosure, loss of privacy, mitigation expense, targeted misuse, completed digital-asset theft, loss of use, and consequential damages.

199. Plaintiffs seek compensatory, consequential, nominal, and other damages, as well as declaratory and injunctive relief, to the full extent permitted by governing law.

COUNT II
BREACH OF IMPLIED CONTRACT
(Against the Global-e Defendants and Ledger on Behalf of Plaintiffs and the Classes)

200. Plaintiffs incorporate the preceding allegations as though fully set forth here.

201. Plaintiffs and Class members entered consumer relationships with Defendants by purchasing Ledger products or associated services, providing payment, and supplying personal and order information necessary to complete and support those transactions.

202. Global-e US Inc. was the seller and merchant of record for U.S. and Canadian transactions, while Ledger continued to operate Ledger.com, provide product and support services, process data, and administer claims. Global-E Online Ltd. operated the integrated platform through which those obligations were performed.

203. An implied term of those transactions was that Defendants would use reasonable measures to protect the information entrusted to them, restrict its use to authorized purposes, retain it no longer than reasonably necessary, provide adequate incident notice, and not expose consumers to unreasonable risks of targeted theft.

204. The implied data-security term was material because a reasonable Ledger customer would not knowingly provide identity, address, and order information if told that Defendants would fail to use reasonable security or would allow the information to identify the customer to organized cryptocurrency thieves.

205. Plaintiffs and Class members performed by paying for products or services and providing accurate information.

206. Defendants breached the implied agreements through the security, retention, oversight, notice, and mitigation failures alleged above.

207. Any contractual exclusion or limitation is inapplicable or unenforceable to the extent alleged above and, in any event, cannot eliminate remedies for duties or misconduct that applicable mandatory law does not permit Defendants to disclaim.

208. The breaches caused Plaintiffs and Class members to suffer the injuries alleged above.

209. Plaintiffs seek contract, consequential, nominal, restitutionary, and other relief available under governing law.

COUNT III
BREACH OF CONFIDENCE
(Against All Defendants on Behalf of Plaintiffs and the Classes)

210. Plaintiffs incorporate the preceding allegations as though fully set forth here.

211. Plaintiffs and Class members conveyed personal, contact, address, order, device, product, purchase, service, and support information to Defendants in confidence and for limited purposes connected to purchasing, fulfilling, supporting, and securing Ledger products and services.

212. The nature of the information, the sensitivity of the Ledger merchant relationship, Defendants' privacy and security representations, and Defendants' roles created a reasonable expectation that the information would be protected from unauthorized access and disclosure.

213. Defendants knew or should have known that unauthorized disclosure would expose consumers to targeted phishing, physical threats, and theft of digital assets.

214. Defendants breached the confidence by failing to maintain reasonable controls and by permitting or failing to prevent the information from being accessed, copied, exfiltrated, disclosed, or used outside the purposes for which it was entrusted.

215. Plaintiffs and Class members suffered the injuries alleged above and are entitled to damages, restitution, an accounting, and equitable relief available under the governing law.

COUNT IV
RESTITUTION / UNJUST ENRICHMENT
(Against All Defendants on Behalf of Plaintiffs and the Classes; Pleaded in the Alternative)

216. Plaintiffs incorporate the preceding allegations as though fully set forth here.

217. Defendants received and retained valuable benefits from Plaintiffs and Class members, including purchase payments, merchant-of-record fees, service revenue, transaction data, consumer information, repeat business, and the commercial value of consumer trust.

218. Defendants also retained the benefit of security, segmentation, minimization, monitoring, notice, and workflow-control expenditures they should have made but allegedly avoided, thereby shifting the resulting costs and risks to consumers.

219. It would be unjust for Defendants to retain those benefits without compensating affected consumers or funding reasonable remediation after failing to provide the security, confidentiality, and incident response that formed part of the exchange.

220. To the extent no enforceable contract governs a particular claim or remedy, Plaintiffs and the Classes seek restitution, disgorgement, an accounting, and other equitable monetary relief permitted by law without duplicative recovery.

COUNT V
DECLARATORY AND INJUNCTIVE RELIEF
(Against All Defendants on Behalf of Plaintiffs and the Classes)

221. Plaintiffs incorporate the preceding allegations as though fully set forth here.

222. An actual and continuing controversy exists concerning Defendants' duties, the reasonableness of their security and notification practices, the scope of the incident, continued retention of compromised information, the adequacy of Ledger's support-verification safeguards, and the measures necessary to reduce ongoing risk.

223. Money damages alone are inadequate because the affected identity, address, merchant-affinity, device, and order information cannot all be changed; the alleged corpus remains capable of repeated enrichment and misuse; and Defendants continue to operate common systems and retain consumer data.

224. Plaintiffs seek a declaration that Defendants owed and breached the duties alleged and must protect, minimize, disclose, and remediate the compromised information consistent with law and reasonable cybersecurity practices.

225. Plaintiffs further seek appropriate injunctive relief, as supported after discovery, requiring independent security assessments; remediation of identified vulnerabilities; reasonable merchant-tenant segmentation; least-privilege access; logging and anomaly detection; data minimization and secure deletion; identification of affected merchants, records, and fields; complete individualized notice; and periodic compliance validation.

226. Plaintiffs also seek reasonable hardening of Ledger's support and Ledger Recover verification workflows, including measures designed to prevent unauthorized third parties from using genuine Ledger communications as proof that an unsolicited caller is legitimate.

227. Plaintiffs seek reasonable monitoring, reporting, and victim-assistance measures for targeted misuse, including preservation and correlation of support, verification, threat-report, and incident records necessary to identify attacks involving compromised customer data.

228. The requested relief is directed to Defendants' common systems and conduct and will benefit the Classes as a whole.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, individually and on behalf of the proposed Classes, respectfully request that the Court enter judgment in their favor and against Defendants and award the following relief:

A. Certify the proposed Classes under Federal Rule of Civil Procedure 23 and any appropriate subclasses or issues; appoint Plaintiffs as class representatives; and appoint their counsel as Class Counsel;

B. Declare that Defendants' acts and omissions alleged herein were wrongful and violated the duties and obligations alleged;

C. Award actual, compensatory, consequential, nominal, restitutionary, and other damages available under governing law, including documented digital-asset losses valued under the legally appropriate methodology;

D. Award restitution, disgorgement, an accounting, and equitable monetary relief to the extent permitted and not duplicative;

E. Award punitive or exemplary damages to the extent authorized and supported by proof developed in discovery;

F. Enter appropriate declaratory and injunctive relief, including the security, segmentation, notice, support-workflow, minimization, deletion, monitoring, and remediation measures described above;

G. Award prejudgment and post-judgment interest;

H. Award reasonable attorneys' fees, litigation expenses, and costs as permitted by law and the common-fund, substantial-benefit, private-attorney-general, or other applicable doctrines;

I. Retain jurisdiction to administer any classwide relief and enforce compliance; and

J. Grant such other and further relief as the Court deems just and proper.

DEMAND FOR JURY TRIAL

Plaintiffs demand a trial by jury on all claims and issues so triable.

Dated: August 24, 2026

Respectfully submitted,

By: *Mark K. Svensson*
Mark K. Svensson, Esq.
MILBERG PLLC
405 East 50th Street
New York, New York 10022
Tel: (202) 975-0468

HALL ATTORNEYS, PC
Nicholas Andrew Hall*
P.O. Box 1370
Edna, Texas 77957
Telephone: (713) 428-8967
Email: nhall@hallattorneys.com

**Pro hac vice* forthcoming

Attorneys for Plaintiffs and the Proposed Classes