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 Kenneth Baylor

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA, SAN FRANCISCO DIVISION

KENNETH BAYLOR, individually and on behalf of all others similarly situated,

Plaintiff,

vs.

LEDGER SAS,

Defendant.

Case No. 26-12867

CLASS ACTION COMPLAINT

1. Breach of Express Warranty
2. CLRA (Injunctive Relief Only)
3. Negligence
4. Strict Liability—Design Defect
5. Strict Liability—Failure to Warn
6. UCL (Injunctive Relief Only)

DEMAND FOR JURY TRIAL

Plaintiff Kenneth Baylor, individually and on behalf of the proposed Class, brings this action against Defendant Ledger SAS. Plaintiff alleges matters concerning his own conduct and experiences on personal knowledge and other matters on information and belief, based on the investigation of counsel, purchase and transaction records, manufacturer publications, and the other facts alleged below.

I. NATURE OF THE ACTION

Ledger sells hardware wallets to protect the secrets that control its customers' cryptocurrency. It designed the hardware, prescribed the packaging and setup process, selected the official distribution channels, and supplied the authentication on which consumers were told to rely. This action arises from Ledger's failure to secure that system against a known threat: concealed spyware that captures recovery information during legitimate setup while the device passes Ledger's Genuine Check. A product purchased to prevent theft instead exposed the information that made the theft possible.

Plaintiff Kenneth Baylor is a California citizen and resident of San Mateo County who purchased his first Ledger device in the United States and used Ledger products from San Mateo County, California, for nearly a decade. Ledger deliberately served that California market, publicly identified San Francisco as a headquarters location, and promoted the Flex product family in this District. In 2026, he followed Ledger's Official Reseller Network to acquire two new Ledger Flex devices from CryptoBilis, which Ledger identified as an official reseller. He used Ledger's official application, received successful Genuine Check results, and generated new recovery information on the devices before committing his assets. His reliance arose from Ledger's continuing security relationship with a California customer and Ledger's own product, distribution designation, and authentication. Ledger's official designation induced Baylor to obtain the products through the channel Ledger presented as protecting their integrity; Genuine Check supplied a separate assurance during setup.

Baylor kept the recovery information offline and did not authorize the transfers at issue. Nevertheless, in October 2026, Bitcoin and Ether with a contemporaneously estimated value of approximately $1.05 million were taken. On information and belief, an unauthorized modification

to one or more of the devices acquired recovery information generated during legitimate setup while leaving the authentic Secure Element able to pass Genuine Check.

Ledger controlled the original hardware design, packaging specifications, authentication protocol, setup instructions, and official reseller designation, including its representations about the integrity of products obtained through that network. It failed to protect the complete recovery-information path, detect and respond to pre-delivery tampering before sensitive operation, provide effective evidence of interference, and disclose the material limits of its successful authentication. Those manufacturer-level failures allowed an altered product to reach a consumer, pass Ledger's prescribed check, and expose newly generated secrets. The identity of the person who installed an implant does not eliminate the causal role of Ledger's original design and its own security assurances.

The challenged failures extend beyond a single reseller. They concern the protection of Ledger hardware throughout manufacturing and assembly, storage, shipping, retail distribution, and returns handling, and the security determination presented when the device reaches its user. Published Nano X implant examinations, Karpelès's reported finding of an implant in a Flex purchased at Singapore Airport, the apparent Stax report, and successive reports from separate MediaMarkt locations support investigation across device families, retailers, and upstream inventory sources. Ledger has also acknowledged a coordinated suspension of MediaMarktSaturn sales while the investigation proceeds. Ledger possesses the product and distribution records needed to identify the affected configurations and points of unauthorized access. Plaintiff seeks relief for one Class of consumer purchasers who lost cryptocurrency through spyware installed in their Ledger hardware wallets before delivery. The Class reaches all Ledger models and sales channels; model-specific examination protocols can account for technical differences without dividing the Class.

Plaintiff seeks compensation for deficient security functionality and the theft of his separately owned cryptocurrency, and preliminary and permanent injunctive relief requiring Ledger to stop the continuing deceptive practices and establish a protective recall, professional inspection, and secure-replacement program. The program must protect Class members against further exposure through their retained or replacement Ledger devices across sales channels. Access must not require

Class members to open their own devices or independently identify an implant before receiving professional assistance. Plaintiff seeks present injunctive relief under the CLRA and California's Unfair Competition Law. He will provide the separate CLRA notice and corrective demand contemporaneously with filing and seek CLRA damages and other remedies subject to Civil Code section 1782 by amendment after compliance with that statute.

II. PARTIES

Plaintiff Kenneth Baylor is a natural person, a United States citizen, and a citizen of California. He is domiciled in and resides in San Mateo County, California.

Baylor purchased the devices for personal use in securing cryptocurrency that he owned. His claim is not brought on behalf of a business. He seeks relief for his own purchases and property losses and for similarly situated members of the Class defined below.

Defendant Ledger SAS is a citizen of France organized under French law. On information and belief, its present principal place of business is in Paris, France. Ledger identifies its address as 106 rue du Temple, 75003 Paris, France.

Ledger designs, manufactures, markets, and distributes Ledger hardware wallets, including the Flex, and supplies the official companion application and Genuine Check. The application is referred to in Plaintiff's records as Ledger Live and in current Ledger publications as Ledger Wallet. This Complaint uses 'Ledger application' for the official companion application and 'Genuine Check' for the authentication at issue.

CryptoBilis sold the two Flex devices to Baylor after Ledger identified that business in its Official Reseller Network as CryptoBilis PH. Ledger SAS supplied the products' original security architecture, packaging specifications, official authentication, and reseller designation. Plaintiff challenges Ledger SAS's own conduct in designing, authenticating, promoting, and distributing the products through the system it created and maintained.

III. JURISDICTION, VENUE, AND DIVISIONAL ASSIGNMENT

Jurisdiction. This Court has original jurisdiction under 28 U.S.C. § **1332(a)(2) (2024).** Plaintiff is a citizen of California, Defendant is a citizen of France, and the amount in controversy on Plaintiff's individual claims exceeds $75,000, exclusive of interest and costs. His

contemporaneous estimate of the cryptocurrency loss is approximately $1.05 million. The Court has supplemental jurisdiction under 28 U.S.C. § 1367 **(2024)** over related class claims within its scope because those claims form part of the same case or controversy.

Ledger purposefully cultivated and served California consumers through direct hardware-wallet sales, delivery to California addresses, collection of California sales tax, and the software, authentication, and security communications accompanying its products. The Ninth Circuit has already recognized that Ledger's California sales, tax collection, and delivery practices constitute purposeful availment of this State: the record before that court included approximately 70,000 wallets sold directly to Californians, generating millions of dollars in revenue. Ledger's own San Francisco headquarters representations and its subsequent promotion of Flex and Stax in this District further demonstrate its deliberate development of the California market. On information and belief, Ledger continues serving that market with the Flex product family and associated product-security services challenged here.[1]

Ledger publicly held itself out as "Headquartered in Paris and San Francisco." In February 2015, Ledger announced the opening of its U.S. subsidiary and San Francisco offices as part of its consumer-product expansion. Its January 18, 2018 financing announcement described an operating team developing cryptocurrency-security products, including its hardware-wallet line, across San Francisco, Paris, and Vierzon. The announcement identified Ledger SAS in its corporate notices. Ledger's 2018 headquarters representation coincided with Baylor's continuing California use of its products. Ledger's California presence was part of its deliberate effort to develop the market for the security products and services at issue.[2]

---

[1] *Baton v. Ledger SAS*, No. 21-17036, 2022 WL 17352192, at *1 (9th Cir. Dec. 1, 2022) (unpublished memorandum; describing the California sales record in that action). *See also Ford Motor Co. v. Mont. Eighth Jud. Dist. Ct.*, 592 U.S. 351, 362–67 (2021).

[2] Ledger, *Ledger Raises USD 75 Million to Secure Cryptocurrency Assets* (Jan. 18, 2018), https://www.ledger.com/ledger-raises-usd-75-million-secure-cryptocurrency-assets (About Ledger and Disclaimers). *See also* Ledger, Ledger Raises a 1.3M€ *Seed* Round to Accelerate the Development of Its Bitcoin Security Solutions (Feb. 19, 2015), https://www.ledger.com/ledger-raises-a-1-3me-*seed*-round-to-accelerate-the-development-of-its-bitcoin-security-solutions

Ledger expanded its U.S. operations before Baylor's 2026 purchases. On March 20, 2026, Ledger announced the opening of a New York City office as part of a multimillion-dollar investment in its U.S. presence, creating dozens of positions across Ledger Enterprise and marketing. Ledger identified the United States as its largest global market, described the office as a strategic hub for its institutional business, and announced John Andrews's appointment as Chief Financial Officer. Chairman and Chief Executive Officer Pascal Gauthier described the initiative as deepening Ledger's U.S. presence. Ledger published a corresponding announcement on its own website on March 23, 2026.[3]

Publicly displayed professional profiles corroborate Ledger's U.S. operating presence. LinkedIn listings reviewed on October 11, 2026 identify Sebastien Badault as SVP Enterprise at Ledger and Andrew Chauvin-DeCaro as Enterprise Marketing Lead at Ledger, each listing the New York City metropolitan area. They identify Dan Panagacos as Senior Technical Account Manager at Ledger, listing New York, New York. The identified executive, marketing, and technical-account functions are consistent with Ledger's announced expansion of its U.S. organization.[4]

Ledger also identifies Portland among its office locations on its official company website.[5] The professional-profile materials identify Isaac Aranda as Wallet Operations Senior Associate at Ledger, listing the Portland, Oregon metropolitan area; Steven Chiboucas as Quality Analyst at Ledger, listing Portland; Jacob Thompson as User Feedback Project Manager at Ledger, listing Beaverton, Oregon; and Quintin Boatwright as Operations Manager and Salesforce Architect at

---

(announcing a U.S. subsidiary and San Francisco offices).

[3] Ledger, *Ledger Appoints New Chief Financial Officer and Opens NYC Office to Scale U.S. Expansion*, Business Wire (Mar. 20, 2026); *see also* Ledger, *New CFO & Opening of NYC Office to Scale U.S. Expansion* (Mar. 23, 2026), https://www.ledger.com/blog-nyc-office-new-cfo (corresponding announcement).

[4] LinkedIn, search-result listings for Sebastien Badault, Andrew Chauvin-DeCaro, and Dan Panagacos (screenshots reviewed Oct. 11, 2026, and preserved in counsel's source file).

[5] Ledger, The Company, https://www.ledger.com/the-company (Our History) (last visited Oct. 11, 2026).

Ledger, listing Vancouver, Washington. Those identified wallet-operations, quality, feedback, and business-systems functions further corroborate Ledger's U.S. operating presence.[6]

Ledger has directed promotion of the product family at issue to San Francisco. In a November 14, 2024 announcement, it identified San Francisco as a planned stop on a tour featuring executive presentations and demonstrations of Ledger Flex and Ledger Stax. Ledger also built a U.S. retail and activation network: its July 18, 2024 announcement described integration of Ledger.com purchases with same-day pickup at Best Buy, in-store educational displays, and guidance through Ledger's own activation materials. Those_activities connect Ledger's consumer marketing, authorized distribution, and manufacturer-prescribed setup into the security system it supplies to its U.S. customers.[7]

Baylor acquired his first Ledger hardware wallet in 2017. Ledger supplied the hardware-security functions used in that continuing California relationship. The relationship included the manufacturer-controlled security system through which Ledger's servers perform its cryptographic genuineness check through the official application. Baylor's 2026 Flex purchases continued his use of that system: he returned to Ledger's own website, followed its official reseller directory, and relied on Ledger's own authentication before entrusting his assets to the new devices. Plaintiff challenges Ledger's own product-security and authentication conduct, not a failure to perform an obligation created by an application-license agreement.

This Court has specific personal jurisdiction over Ledger under Federal Rule of Civil Procedure 4(k)(1)(A) and California Code of Civil Procedure section 410.10. Baylor's claims arise out of and relate to Ledger's sustained California business in the same hardware wallets, manufacturer-supplied authentication, and security assurances challenged here. Ledger developed

[6] LinkedIn, search-result listings for Isaac Aranda, Steven Chiboucas, Jacob Thompson, and Quintin Boatwright (screenshots reviewed Oct. 11, 2026, and preserved in counsel's source file).

[7] Ledger, Global Tour announcement (Nov. 14, 2024), https://www.ledger.com/ledgers-global-tour-celebrating-10-years-of-secure-digital-ownership (last visited Oct. 11, 2026). *See also* Ledger, *Ledger and Best Buy Launch Same-Day Pickup for Online Customers in the US* (July 18, 2024), https://www.ledger.com/blog-ledger-and-best-buy-launch-same-day-pickup-for-online-customers-in-the-us.

and served a California market for Flex devices and its official application, promoted Flex in this District, and maintained the continuing hardware-security relationship with Baylor described above. Baylor obtained the two Flex devices to continue using Ledger's security products and relied on Ledger's official reseller designation and Genuine Check. His claims challenge Ledger's own design, packaging, authentication, warnings, and distribution controls supplied through that continuing consumer relationship.

The exercise of jurisdiction accords with fair play and substantial justice. Ledger deliberately built a substantial California consumer business, publicly identified San Francisco as a headquarters location, and promoted the Flex product family here. Its announced U.S. expansion and publicly identified executive, marketing, technical-account, wallet-operations, quality, and customer-feedback functions demonstrate a substantial U.S. operating presence. Ledger has described the United States as its largest global market and committed additional capital and personnel to serving it. California has a substantial interest in protecting its resident consumers and their separately owned property from the alleged failure of security products marketed to them. Ledger possesses or controls the product specifications, authentication records, distribution requirements, and organizational evidence needed to adjudicate these claims.

Venue is proper under 28 U.S.C. § 1391(c)(3) (2024), because Ledger SAS is a defendant not resident in the United States. Ledger's California consumer business, public San Francisco headquarters representations, promotion of the product family at issue, and Baylor's longstanding California relationship with Ledger connect this action to this District.

Divisional Assignment. Assignment to the San Francisco or Oakland Division is appropriate under Civil Local Rules 3-2(c)–(d) and 3-5(b). Plaintiff is domiciled in San Mateo County, California, and his longstanding use of Ledger products occurred in that county. The California course of dealing and consumer relationship alleged here concerns a county served by those Divisions.

Plaintiff's California consumer claims enforce nonwaivable rights and class remedies under Civil Code sections 1751 and 1781 and California Business and Professions Code sections 17200 *et seq.* California has a fundamental interest in protecting its resident consumers from the challenged

practices of a manufacturer that deliberately serves this State. Plaintiff *see*ks enforcement of those protections in his home forum.

IV. FACTUAL ALLEGATIONS

A. Ledger supplies the product and the initial security determination

A hardware wallet generates and protects private keys used to authorize transactions involving cryptocurrency recorded on a blockchain. A recovery phrase permits those keys to be reconstructed on a compatible wallet. Anyone who obtains the necessary recovery information can gain control of the associated assets without possessing the owner's original device.

The cryptocurrency belongs to the user independently of the hardware wallet. Ledger did not sell Plaintiff the Bitcoin or Ether lost in this incident. The Flex was purchased to secure the credentials controlling that separately owned property.

Ledger supplies its hardware wallets together with an official setup process, security instructions, and companion application. The product family uses a manufacturer-controlled Genuine Check directed to the Secure Element. A successful result is presented during the prescribed setup process and informs the purchaser's decision whether to entrust cryptocurrency to the device. The relationship between that component authentication and the integrity of the complete recovery-information path is a common issue across models using the challenged process. Ledger's developer documentation lists the same microcontroller and Secure Element models for Flex and Stax and describes a separate microcontroller handling peripheral communications for the Secure Element.[8]

Ledger's current Flex setup guide places Genuine Check before generation of a new 24-word recovery phrase, consistent with Plaintiff's reported sequence. The guide bears a January 6, 2026 publication date and an October 9, 2026 update date.[9]

---

[8] Ledger, Hardware Architecture, Ledger Developer Portal (updated Sept. 23, 2026), https://developers.ledger.com/docs/device-app/explanation/ledger-os/hardware-architecture (Flex and Stax component table; Secure Element proxy architecture).

[9] Ledger, Unboxing Your Ledger Flex: A Step-by-Step Guide to Secure Digital Ownership (Jan. 6, 2026; updated Oct. 9, 2026), https://www.ledger.com/academy/topics/ledgersolutions/unboxing-

The same guide describes the two strips of tape on a Flex box as serving packaging purposes and directs purchasers to the security built into the device and the setup check. Ledger thus directs the purchaser to rely on the product's security architecture and authentication to evaluate a newly received Flex, while the supplied paper closures provide no device-linked assurance against opening and resealing.

Ledger's published technical description explains that its server challenges the device's Secure Element and verifies its cryptographic response and attestation. This process can establish that the original Secure Element is genuine. It does not, by itself, establish that every part of the device remains physically unmodified.

Ledger's Donjon threat-model documentation expressly recognizes that a successful Genuine Check may coexist with an unauthorized physical spying implant if the original Secure Element remains intact. It also distinguishes authenticity from verification of the device's physical supply-chain history. An attacker who acquires the recovery information elsewhere in the device can bypass the protection afforded by authenticating the original chip.[10]

Ledger states in its current consumer buying guide that Genuine Check "cannot detect unauthorized physical modifications to the hardware—such as spying implants—if the original Secure Element remains intact." In its discussion of counterfeit devices and counterfeit companion software, the same guide directs: "No visual inspection, no packaging check, no seller reputation can substitute for running the Genuine Check yourself with authentic software." It also acknowledges that "no global supply chain is entirely immune to highly sophisticated interception or tampering attacks." These statements confirm Ledger's distinction between a necessary component-authentication step and an assessment of the complete device. Baylor followed the

your-ledger-flex-a-step-by-step-guide-to-secure-digital-ownership (last visited Oct. 11, 2026).

[10] Ledger Donjon, *Genuineness* - Threat Model, https://donjon.ledger.com/threat-model/device-genuineness/ (last visited Oct. 11, 2026).

prescribed authentication, yet the setup did not tell him that a successful result left the alleged physical interception path unresolved before he generated recovery information.[11]

That distinction matters at the point of initial use. A purchaser deciding whether to generate a recovery phrase on a newly acquired device needs to know whether the manufacturer's successful result addresses an alteration capable of exposing that phrase. A result verifying only an authentic component does not supply that answer if a separate implant can remain undetected.

Ledger controls the language of its successful result and the warnings and instructions displayed during setup. It can explain material limits before the purchaser generates recovery information or commits assets. Plaintiff alleges that the setup presented to him did not adequately disclose the implant limitation at that decision point. The warning needed to accompany the successful result on which Ledger directed him to act, before the device generated the secrets controlling his assets.

A supply-chain compromise, as used here, is an unauthorized addition, substitution, or alteration of hardware or device-resident code before delivery to the consumer that acquires recovery information generated during legitimate setup or defeats the protection of that information through the delivered device. The spyware may include an added circuit, substituted component, modified display assembly, or code carried by an unauthorized component. The relevant chain includes component sourcing, manufacturing and assembly, storage, shipment, distribution, retail custody, and returns. Plaintiff alleges that Ledger's original protective design and verification system permitted the compromise to expose recovery information while the original Secure Element remained authentic. Identification of the precise insertion point requires the physical and distribution evidence within Ledger's and the supply-chain participants' possession.

[11] vineet.nair, *Best Practices To Securely Buy Your Ledger Signer*, Ledger (Mar. 6, 2026, updated Sept. 18, 2026), https://www.ledger.com/academy/topics/ledgersolutions/best-practices-to-securely-buy-ledger-signer, under "Ledger Genuine Check: Explained" and "Counterfeit Devices" (last visited Oct. 19, 2026; current publication, not proof of purchase-date exposure).

B. Ledger represents the integrity of products supplied through its official network

Ledger maintains an Official Reseller Network on its website, organized by location and identifying businesses from which consumers may obtain Ledger products. The designation is Ledger's own statement about the seller's place in its authorized distribution channel.

Ledger's own website describes its authorized-channel protections in *Best Practices To Securely Buy Your Ledger Signer*. Under its discussion of supply-chain security, Ledger describes its retail partners as "carefully selected Authorized Resellers" and says they are "commercially incentivized" to obtain inventory directly from Ledger or its authorized distributors. It describes a "vetted logistics pipeline" designed to mitigate third-party-wholesaler and grey-market sourcing risks, and states that its distribution agreements prohibit partners from restocking and reselling returned devices. It also maintains an official reseller registry and recommends its own store or listed resellers to enhance authenticity and supply-chain integrity. [12]

These are representations about protective practices applied to the goods and their distribution, not merely permission to use Ledger's name. In the security context alleged here, Plaintiff understood Ledger's official purchasing designation to identify a channel whose selection, sourcing, and custody protections made the delivered product suitable for secure initialization. Ledger's current guide corroborates that manufacturer-described function and informs the challenge to its continuing practices; the purchasing representation Baylor actually encountered was Ledger's designation of CryptoBilis in its own directory. Plaintiff's theory concerns the product-integrity meaning conveyed in that context, independently of the later authentication of the Secure Element.

Ledger created and controls its official distribution system. It selects participating resellers, maintains the registry and purchasing links, establishes sourcing incentives, and, according to its own guide, contractually prohibits distribution partners from restocking and reselling returned devices. Those measures address opportunities for substitution, unauthorized physical access, and recirculation of compromised products. On information and belief, Ledger's relationship with

[12] vineet.nair, *Best Practices To Securely Buy Your Ledger Signer*, Ledger (Mar. 6, 2026, updated Sept. 18, 2026), https://www.ledger.com/academy/topics/ledgersolutions/best-practices-to-securely-buy-ledger-signer, under "Ledger Supply Chain: How Ledger Distribution aligns with security industry standards" (last visited Oct. 19, 2026).

CryptoBilis included arrangements for distributing Ledger products. The governing requirements, audits, sourcing records, and enforcement communications are within Ledger's and the distributor's possession. [13]

Ledger joined two consumer decisions into its prescribed security process: where to obtain a device and whether to trust the delivered hardware. It designated the official seller and supplied the successful initial authentication. Ledger knew purchasers would rely on both before generating recovery information and committing assets. Reasonable performance of those retained functions required security controls throughout the authorized channel, reliable inventory provenance, protection against returned-product substitution, and revalidation when the ownership or operation of an authorized seller materially changed. Ledger's written product-integrity assurances and its designation of the seller are distinct from, and cumulative with, the device-specific authentication supplied during setup.

In a public statement concerning CryptoBilis, Arravind Prabu stated that CryptoBilis had been acquired by new ownership and that he and Vimalatheethan completed a handover of operational, managerial, and administrative responsibilities in March 2026. He further stated that suppliers had been notified of the acquisition and new management, while contractual restrictions postponed a joint public announcement until mid-October 2026. The statement identifies Nicholas Chang as the current operational contact.[14]

That reported transition preceded both of Baylor's purchases. On information and belief, Ledger received notice of the ownership or management change as a supplier to the authorized distribution network. It nevertheless continued to present CryptoBilis as an official source when Baylor selected it. On information and belief, Ledger failed reasonably to revalidate the operator, custody of authorized inventory, access to stock, returns handling, and compliance with the security requirements associated with its designation before continuing to direct consumers to that business.

[13] *Id.*, under "Ledger Supply Chain: How *Ledger* Distribution aligns with security industry standards" (describing sourcing incentives and a contractual prohibition on resale of returns).

[14] Arravind Prabu, *Official Statement Regarding CryptoBilis*, LinkedIn, numbered items 1, 2 & 4 (undated post reproduced in screenshot supplied by Plaintiff; copy on file with counsel).

A screenshot Baylor captured on October 11, 2026 shows CryptoBilis PH still displayed in Ledger's Official Reseller Network with a purchasing link and no warning adjacent to that entry, after Ledger's October 10 public acknowledgment of a hardware implant. By October 12, CryptoBilis PH no longer appeared in the official Philippines reseller list. Ledger controlled that consumer-facing designation and its revision. Changing the directory did not examine hardware already delivered to consumers, identify all affected inventory, or resolve the common limitations of Ledger's prescribed security check.[15]

C. Baylor's history, purchases, and reliance

In 2017, Baylor acquired a Ledger hardware wallet in the United States and subsequently used it from San Mateo County, California, for nearly a decade without experiencing a compromise of the assets he secured with it. His longstanding experience with Ledger's products and security system led him to return to Ledger when he needed another device.

In July 2026, Baylor visited ledger.com to obtain another Ledger device. Ledger's website directed him to its Official Reseller Network, where he selected CryptoBilis and followed the purchasing process. Ledger's official designation materially influenced his choice. Baylor remained a California citizen and domiciliary throughout the purchases and the loss alleged here. He relied on Ledger's designation in choosing the authorized channel to obtain an authentic, unmodified Ledger product, rather than treating the directory as a list of unrelated sellers. His reliance on that purchasing representation preceded and was distinct from his reliance on Genuine Check during setup.

On July 13, 2026, Baylor purchased a new Ledger Flex in BTC Orange from CryptoBilis. He selected the product through the official distribution channel Ledger identified.

On September 4, 2026, Baylor purchased a second new Ledger Flex, in Oxidate Green, from the same Ledger-designated seller.

[15] Ledger, *Official Reseller Network*, Philippines listing, https://shop.ledger.com/pages/resellers?continent=asia+%26+oceania&country=philippines (Plaintiff's Oct. 11, 2026 screenshot on file with counsel).

Baylor paid approximately $620.00 for the two transactions and received products sold as new. The purchase records identify him as the purchaser. The security architecture, packaging, official application, and Genuine Check supplied with both products came from Ledger.

Baylor received the Flex devices in retail packaging secured by two ordinary paper strips. The closures did not have individualized serial identifiers, holographic features, or destructive void adhesive. He observed no visible indication that the delivered products had been physically compromised.

For setup, Baylor connected the devices to Ledger's official application and ran Genuine Check. He received successful results identifying the devices as 'Genuine.' He relied on those results before proceeding with generation of new recovery information and committing cryptocurrency to accounts controlled by that information.

Baylor generated the recovery information natively on the devices. He did not use a recovery phrase supplied by the reseller or written in advance by another person. He kept the recovery information offline, did not digitize it, did not store it in a cloud service, and did not enter it into an Internet-connected interface.

In the context of a new Flex obtained through Ledger's official reseller channel and the prescribed setup sequence, Baylor understood the successful result as confirmation that the particular device had satisfied Ledger's authentication for secure initialization and use. The affirmation concerned the existing security condition of the product on which he was about to generate the secrets controlling his assets. Ledger's earlier representation about the integrity of products obtained through its official channel independently informed that understanding. The two assurances addressed different stages of the same purchase and initial use.

Before Baylor proceeded, Ledger did not adequately tell him in that setup process that a device could pass while containing a physical implant capable of obtaining newly generated recovery information. He was not warned that his adherence to the official channel and a successful result left that specific, concealed condition unresolved. Nor did the purchasing process adequately explain that Ledger's official designation did not establish that the particular delivered device was

free from a concealed physical alteration capable of capturing newly generated recovery information.

Baylor would not have generated recovery information on an affected device or placed his assets under the control of that information had the relevant condition or limitation been adequately disclosed before funding. He would have withheld the assets pending a secure alternative. Had Ledger adequately disclosed that its designated purchasing channel left that condition unresolved, Baylor would have withheld the purchase or obtained a securely verified alternative before entrusting assets to the delivered hardware.

After setup, Baylor placed Bitcoin and Ether under the control of the new recovery information. He owned the cryptocurrency transferred without authorization in the incident alleged below.

D. The unauthorized transfers and alleged physical compromise

On or about October 9, 2026, cryptocurrency controlled through the affected recovery information was transferred without Baylor's authorization. The unauthorized transactions depleted 10.66256803 BTC and 58.991906189521260209 ETH from his assets, inclusive of the associated network transaction fees.

Baylor contemporaneously estimated his total loss at approximately $1.05 million. The legally recoverable dollar value of the asset quantities alleged above will be established according to proof under the applicable valuation measure. Plaintiff seeks a single recovery for each loss, including any associated network fees.

Baylor promptly quarantined the affected hardware and retained purchase documents and transaction records. He did not authorize the transfers, and he did not knowingly disclose his recovery information to the recipients or approve transfers to them.

Before filing, Baylor reported the unauthorized losses to Ledger. On October 12, 2026, Ledger Support responded in case 00285187 and instructed him to move any remaining funds associated with his current recovery phrase to a new recovery phrase without using the current device. To investigate, Ledger requested the serial identifiers on the box, on the back of the device, and in the firmware, where available; the purchase and delivery records; packaging photographs;

setup history; firmware information; and application logs. That response identifies the product-identity, provenance, and configuration information Ledger itself considers relevant to investigating the reported compromise.

On information and belief, one or more of the Flex devices were physically altered before delivery to Baylor, in a manner that permitted capture of recovery information generated during legitimate setup while preserving the authentic Secure Element and its ability to pass Genuine Check. Plaintiff alleges that this compromise enabled the unauthorized transfers.

The grounds for that inference include Baylor's native generation and offline handling of recovery information; the successful manufacturer checks; the subsequent unauthorized depletion of assets; and the documented physical implant attacks on Ledger hardware that can leave component authentication intact. On information and belief, an unauthorized component acquired recovery information through the device's display or associated circuitry before the resulting theft. The product's original susceptibility to that interference and Ledger's misleading security determination operated together. The precise implant configuration and point of insertion can be established through examination of the preserved hardware and the manufacturing, attestation, batch, custody, and distribution records.

The original design failed to make the recovery-information path sufficiently resistant to foreseeable interference or to prevent sensitive initialization after that path had been compromised. The enclosure, component protections, packaging, authentication scope, and user-facing security determination operated together. Their inadequacy allowed the alleged malicious addition to defeat the product's security purpose without an effective warning to Baylor before he exposed his assets.

On information and belief, the absence of durable, individualized indications of interference with the packaging and enclosure facilitated opening, alteration, and resealing without a warning visible to Baylor. The ordinary paper closures neither authenticated the package's relationship to the enclosed device nor supplied a persistent indication of earlier access. Those deficiencies left Baylor dependent on the device and Ledger's check to identify concealed interference.

Acquisition of the recovery information and theft of the associated assets were foreseeable consequences of this alleged condition. A malicious effort to intercept a device or acquire its

recovery information is a hazard for which purchasers obtain a security product. Ledger knew that the value of cryptocurrency controlled by a device could substantially exceed the device's purchase price.

On information and belief, effective physical barriers or a verifiable indication of prior opening would have prevented or exposed the interference before use; a tamper response that blocked sensitive initialization would have prevented the compromised device from revealing new recovery information; and an adequate warning would have caused Baylor to withhold his assets. Each protection addressed a stage of the sequence that led from concealed pre-delivery alteration to unauthorized transfer.

E. Knowledge of the risk and common design choices

Ledger designed the authentication and knew which components and conditions it did and did not examine. On information and belief, before Plaintiff's purchases, Ledger knew that authentic-component verification did not itself exclude an additional physical implant, and that users could mistake a successful result for resolution of that risk unless the distinction was adequately explained.

Ledger had publicly identified supply-chain substitution and resealing risks years earlier. In March 2019, its Donjon team described opening a competitor's package, altering a device, and resealing the package despite a security sticker. Ledger also described the risk that attackers could return altered devices into a manufacturer's sales channel. Ledger's own analysis thus recognized that physical access, packaging, returns handling, and device design had to be evaluated together.[16]

Physical implants in Ledger hardware had been examined before Baylor's purchases. Security researcher Joe Grand published an analysis of an implant in a Ledger Nano X, with presentation materials revised May 29, 2026. The work documents an unauthorized physical

[16] Ledger, *Our Shared Security: Responsibly Disclosing Competitor Vulnerabilities* (Mar. 11, 2019), https://www.ledger.com/our-shared-security-responsibly-disclosing-competitor-vulnerabilities.

addition to Ledger hardware and the recovery-information interception risk posed by a compromised device.[17]

On October 10, 2026, Tai Zen publicly stated that he had sent multiple tampered Ledger devices to Ledger's Donjon security team in January 2026. Mark Karpelès quoted that statement publicly on October 11, 2026. The reported submission preceded Baylor's purchases and supports Plaintiff's allegation, on information and belief, that Ledger had received specific notice of physical tampering in its distribution chain.[18]

The reported notice was not limited to general research. On October 16, 2026, security researcher Joe Grand told Cointelegraph that he alerted Ledger on March 4, 2026 to a malicious implant in a Nano X purchased through Lazada Thailand in August 2025. According to Grand, Ledger acknowledged the findings and said it was investigating internally; he criticized its failure to warn customers proactively. Karpelès separately reported awareness of at least two contacts beginning in December 2025. The article did not establish the marketplace seller's authorization when that device was purchased. The significance here is notice to Ledger of an actual implant mechanism before both of Baylor's purchases, not an allegation that Grand's specimen came from an authorized seller.[19]

On October 10, 2026, Ledger publicly confirmed that one impacted user's device contained an unauthorized hardware implant and stated that it was contacting affected users as part of its

[17] Joe Grand, *Reverse Engineering a Ledger Nano X Hardware Implant*, Grand Idea Studio, presentation slides 72–73, 77 (rev. May 29, 2026), https://grandideastudio.com/portfolio/security/ledger-hardware-implant/ (presentation linked on the project page).

[18] Tai Zen (@HeyTaiZen), X (Oct. 10, 2026), quoted in Mark Karpelès (@MagicalTux), X (Oct. 11, 2026), https://x.com/MagicalTux/status/2109272516544041066 (reproduced post stating that devices were sent in January 2026; screenshot on file with counsel).

[19] Helen Partz, *Ledger's Early Implant Warnings Deserved More Action, Karpelès Says*, Cointelegraph (Oct. 16, 2026), https://ct.com/news/ledger-early-implant-warnings-mark-karpeles (reporting interviews with Grand and Karpelès; *see also* "Marketplace Listings Expose Reseller Verification Gaps").

investigation. That acknowledgment corroborates the occurrence of physical implants in delivered Ledger hardware.[20]

On October 11, 2026, Ledger directed CryptoBilis purchasers not to initialize unused devices and advised users who had already completed setup to move to a new seed on a device obtained from Ledger. It reminded its authorized resellers and distributors to source products only through authorized channels and never restock returned devices, and announced review of reseller controls and hardware protections. Ledger described the confirmed cases in its then-current investigation of the October 9 incident as involving CryptoBilis. That account of the cases then confirmed did not identify the manufacturing, custody, and examination evidence needed to resolve the separate implant reports described below or the common limitations of Ledger's authentication. Plaintiff alleges that Ledger's original security failures and the necessary corrective relief extend beyond that reseller.[21]

In an October 2026 field report, Tibane Labs described two implanted Ledger Nano X specimens obtained in September 2026: one through Yahoo! Auctions in Japan, and one from a China-based seller on Amazon Japan, shipped from Malaysia. Tibane reported added circuitry connected to the display path and cellular communication components. In the newer specimen, black-coated circuitry was concealed beneath the OLED display while the original battery remained in place.[22]

On October 10, 2026, Mark Karpelès published comparative photographs of Nano X implant configurations and identified connections to display-bus signals at the device's factory test pads. He described the newer black configuration as using fewer tapped signals than an earlier version and

[20] Ledger Support (@Ledger_Support), X (Oct. 10, 2026), https://x.com/Ledger_Support/status/2108968264055345381 (statement concerning an implant in one affected user's device).

[21] Ledger (@Ledger), X (Oct. 11, 2026), https://x.com/Ledger/status/2109331538072494364 (72-hour update; instructions to CryptoBilis customers and authorized distribution partners).

[22] Tibane Labs, *Ledger Nano X: The Spy Implant* (Oct. 2026), https://www.tibane.net/research/ledger-nano-x-implant.

inferred that this simplified installation. These reported physical connections further support an interception path outside the genuine Secure Element.[23]

On October 11, 2026, a user posting as @0xJohannes_ reported an apparent implant in a Ledger Nano X purchased in person through a European retailer and identified MediaMarkt in a follow-up. Public posts by Coin Academy, Crypto Banter, and @RatPoisonaut reproduced the report and the same photograph of the opened device.[24] Later that day, the same account published a closer photograph showing the apparent added assembly and antenna lead. Mark Karpelès publicly identified the first photographed assembly as another spy implant resembling an earlier iteration of the implant he was examining. The report and that technical assessment identify an additional alleged compromised Ledger product obtained through a different retail channel.[25]

On October 12, 2026, Johannes reported finding an apparent spyware implant in a second Ledger device purchased that day at a different MediaMarkt location. He published photographs and linked a video he described as recording the unboxing, and reported the same additional wiring and LTE module in the newly purchased device. He further reported that a MediaMarkt employee told him this device was not a customer return and that returned Ledger devices were sent back to the manufacturer rather than resold. He identified store inventory records as showing Aqipa GmbH as the source of the stock.[26]

---

[23] Mark Karpelès (@MagicalTux), X (Oct. 10, 2026), https://x.com/MagicalTux/status/2109031679528702257 (comparative photographs and discussion of display signals and test-pad connections).

[24] Johannes (@0xJohannes_), X (Oct. 11, 2026), https://x.com/0xJohannes_/status/2109240472933671125; Johannes (@0xJohannes_), X (Oct. 11, 2026), https://x.com/0xJohannes_/status/2109285908079915305 (follow-up identifying MediaMarkt; preserved reproductions on file with counsel).

[25] Johannes (@0xJohannes_), X, photograph 2 (Oct. 11, 2026), https://x.com/0xJohannes_/status/2109369736391794711/photo/2; *see also* Mark Karpelès (@MagicalTux), X (Oct. 11, 2026), https://x.com/MagicalTux/status/2109249759508869184 (assessment of the earlier European-device photograph).

[26] Johannes (@0xJohannes_), X (Oct. 12, 2026), https://x.com/0xJohannes_/status/2109634513957527974 Johannes (@0xJohannes_), X (Oct. 12, 2026), https://x.com/0xJohannes_/status/2109634517296148568 (accompanying video post;

Aqipa independently announced its Ledger distribution partnership in Germany and Austria in August 2023, identifying the Nano X among the products. Ledger's own German consumer guide identifies MediaMarkt as an authorized retail partner. The successive reports therefore implicate another authorized retail channel and a separately identified upstream distributor. They support tracing inventory through the distribution chain and comparing production lots, device configurations, and access to stock across stores, rather than confining the inquiry to a single retail seller.[27]

On October 13, 2026, Ledger announced that MediaMarktSaturn had suspended sales of Ledger devices in stores and online in coordination with Ledger following a German customer's report of a hardware implant. A MediaMarktSaturn spokesperson separately confirmed removal of Ledger products from the retailer's lineup in all countries as a precaution. Ledger stated that no fund loss had been reported in that German case and that it had no indication its infrastructure, systems, or services were compromised. The sales suspension extended beyond CryptoBilis; it did not itself inspect devices already delivered to consumers.[28]

On October 11, 2026, the account @wentrre posted three internal photographs of a device it identified as its Ledger Stax and asked Ledger whether the device had a problem. The photographs show a Ledger-marked board with an apparent additional assembly, including a component marked Nordic Semiconductor nRF9151 and a cable leading toward the rear cover. Bitcoin News reproduced the post that day and characterized the assembly as suspected unauthorized hardware.[29]

---

purchase, inventory provenance, and retailer statements are attributed to the reporting user).

[27] Aqipa, Aqipa started mit LEDGER in neuer Kategorie der Krypto Wallets (Aug. 2, 2023), https://inside.aqipa.com/de/news/posts/aqipa-started-mit-ledger-in-neuer-kategorie-der-krypto-wallets (article dateline Aug. 1, 2023); Ledger, *Crypto in Germany: The Ultimate Guide*, https://www.ledger.com/academy/topics/country-guides/crypto-in-germany-the-ultimate-guide (current text identifying authorized retailers).

[28] Ledger (@Ledger), X (Oct. 13, 2026), https://x.com/Ledger/status/2109984923343782374, quoted in Helen Partz, *MediaMarktSaturn Pulls Ledger Products Amid Tampering Reports* (Oct. 13, 2026), https://cointelegraph.com/news/mediamarkt-pulls-ledger-wallet-security-incident (quoting Ledger's statement and a MediaMarktSaturn spokesperson).

[29] @wentrre, X, photographs 1–3 (Oct. 11, 2026),

Mark Karpelès also linked the original report and identified the pictured Stax as apparently containing an implant. Nordic Semiconductor identifies the nRF9151 as incorporating an LTE-M/NB-IoT cellular modem.[30] The suspected assembly's function and the circumstances of that device's delivery remain unverified.

On October 13, 2026, Mark Karpelès reported finding a spy implant in a Ledger Flex purchased at Singapore Airport. His post identified Ben Yorke as the owner, stated that Yorke noticed suspicious marks and withheld the device from use, and linked an inspection video. This reported finding concerns the same product model purchased by Baylor and a different retail channel. It supports tracing Flex inventory and comparing the relevant product configurations across sellers and upstream suppliers rather than limiting the inquiry to the CryptoBilis transactions.[31]

The Nano X examinations, the reported Flex implant from a Singapore Airport purchase, the apparent Stax assembly, and the repeated European retail reports support a manufacturer-wide inquiry into susceptibility to pre-delivery alteration and the limits of Ledger's security check. The reported Flex finding supplies same-model evidence relevant to Baylor's claim without establishing that every specimen has an identical alteration or that all were compromised at the same point in the supply chain. The reported involvement of new inventory from an identified distributor makes the sourcing, lot, and custody records upstream of the retail store material to determining the reach of

---

https://x.com/wentrre/status/2109339646102778306; Bitcoin News (@BitcoinNewsCom), X (Oct. 11, 2026), https://x.com/BitcoinNewsCom/status/2109379275325309107 (reproducing the same owner's photographs, not a separate incident).

[30] Mark Karpelès (@MagicalTux), X (Oct. 11, 2026), https://x.com/MagicalTux/status/2109370197710868656 (commenting on the @wentrre photographs); Nordic Semiconductor, nRF9151, https://www.nordicsemi.com/Products/nRF9151 (component documentation; modem capability does not establish operation of the pictured assembly); *see also* Ariel Givner (@GivnerAriel), X (Oct. 11, 2026), https://x.com/GivnerAriel/status/2109418373377638688 (commentary on the same reported specimen).

[31] Mark Karpelès (@MagicalTux), X (Oct. 13, 2026), https://x.com/MagicalTux/status/2109916873689280900, reproduced in Kim Zetter, *Who Is Planting Backdoors in Ledger Crypto Wallets?* (Oct. 13, 2026), https://www.zetter-zeroday.com/who-is-planting-backdoors-in-ledger-crypto-wallets/ (attributed account of the Singapore-airport Flex; not a verified report of asset theft from that specimen).

the compromise. An implant that captures display information and has its own cellular connection can expose recovery information even when the owner keeps the phrase off networked computers. Ledger applies the Secure Element authentication principle across its product family, and its own technical documentation identifies common core components in Flex and Stax. Its original design records, incident submissions, product examinations, manufacturing and shipment records, and reseller controls provide common evidence of which devices share the challenged condition. The scope of protective relief should follow that evidence, rather than the identity of the last seller or the first incident Ledger publicly confirmed.

Ledger's knowledge of the authentication it designed, its earlier supply-chain research, the published implant analysis, and the reported submission of tampered devices and acknowledgment of Grand's March 4, 2026 disclosure establish a factual basis for its pre-purchase knowledge of the risk. On information and belief, Ledger knew before Baylor's purchases that its successful check could leave a concealed interception path unresolved, yet failed to implement adequate physical protection, tamper response, packaging controls, and point-of-use disclosure. The resulting exposure was the foreseeable failure of the security function for which consumers bought the product.

On October 15, 2026, Ledger published a further response. It reported reverse-engineering the implant, examining spot-purchased and warehouse samples, finding those sampled stock units clean, and asking authorized resellers and distributors to suspend sales in Southeast Asia and Hong Kong. It denied a flaw in its chip, operating system, or servers and characterized the event as a localized distribution attack. Ledger also announced immediate instructions to keep products off shelves and displays, hold stock in backrooms until sale, prohibit all resale of returns, and escalate unusual-product reports. It stated that additional product-level measures were being developed. These measures addressed selected inventory and future handling; the announcement did not establish a comprehensive inspection or verified-replacement program for products already held by Class members.[32]

[32] The Ledger Team, *Ledger's Response to the Hardware Implant Attack*, Ledger (Oct. 15, 2026), https://www.ledger.com/blog-response-hardware-implant-attack, under "What Happened," "How We Responded," and "What We Are Doing Differently."

The same day, Ledger's Chief Technology Officer, Charles Guillemet, expressly acknowledged that "an attestation cannot catch an implant spying on the screen." He stated that "over the past few months" Ledger had developed an active shield around the new Ledger Atom's secure zone to detect pre-delivery touching, opening, probing, or modification and trigger a Secure Element response. This account places protective engineering before the October 9 losses and confirms Ledger's awareness that authenticating the chip does not resolve screen interception. The precise development milestones, test results, and applicability to the earlier devices are within Ledger's records.[33]

Ledger's Atom whitepaper describes a protected enclosure for the Secure Element, graphics coprocessor, and display-switch circuitry; display-signal tracks buried within the circuit board; and a second opening-detection perimeter resettable only through a controlled Ledger-supervised process. It separately describes isolating the sensitive screen and touch input from compromised Android software. A Ledger spokesperson told The Block that the announced tamper sensors would have an independent battery and stated: "The Core Protection feature will explicitly block the screen reader implants from this weekend's incident." These are Ledger's announced design and performance claims, not results of an independent examination of Baylor's Flex devices.[34]

The launch also addressed packaging and distribution. Solana Mobile's October 15 partnership announcement described planned tamper-resistant and tamper-evident measures extending from Atom's packaging to the device and stated that Atom would be sold directly through

[33] Charles Guillemet, *The Security Architecture of Ledger Atom™*, Ledger (Oct. 15, 2026), https://www.ledger.com/blog-ledger-atom-security-architecture, under "Privacy & Tamper Protection Are Built Into the Hardware."

[34] Ledger, *Ledger Atom™—Whitepaper* (Oct. 15, 2026), https://www.ledger.com/ledger-atom-whitepaper, under "Secure Screen," subsections "Physical Tamper Protection" and "Display and Touch Isolation"; James Hunt, *Ledger Unveils Atom Android Device with Solana Mobile Integration and New Tamper Protections Amid Investigation into Modified Wallets*, The Block (Oct. 15, 2026), https://www.theblock.co/news/business/2026-10-15-ledger-atom-solana-mobile-418644, under "Protections Against Physical Tampering" (quoting Ledger's spokesperson).

Ledger's official site. These statements identify physical custody, enclosure integrity, and packaging as distinct protections in addition to Secure Element authentication.[35]

Ledger marketed Atom as a smartphone-shaped, Android-based security device; its product FAQ specifies that it is a data-only device, not a conventional cellular telephone. The October 15 announcement solicited a $100 refundable reservation toward an $849 reserve price and projected delivery in 2027, while disclosing that Atom remained in development and its design, features, price, and delivery estimate could change. The same announcement encouraged people who did not already own a Ledger to buy one immediately. A reservation for a future product was not an immediately available correction of hardware already sold.[36]

CoinDesk also reported Ledger's statement that it had no plans for a trade-in program for existing customers affected by the incident, although future upgrade promotions were not excluded. That statement concerns trade-ins; it is not an allegation that Ledger denied every form of support. The distinction remains material to the relief sought: announcing additional security for a future premium product, restricting retail handling, and offering case-specific support do not establish the integrity of every Covered Device already held by Class members or provide the court-supervised corrective program alleged below.[37]

---

[35] Solana Mobile, *Solana Mobile Announces Ledger as Its First Hardware Expansion Partner*, PR Newswire (Oct. 15, 2026), https://www.prnewswire.com/news-releases/solana-mobile-announces-ledger-as-its-first-hardware-expansion-partner-302909677.html (announcing packaging-to-device tamper protections and direct-site distribution).

[36] Pascal Gauthier, *Ledger Atom™: The Device Built to Protect Everything You Value*, Ledger (Oct. 15, 2026), https://www.ledger.com/blog-introducing-ledger-atom, under "Ledger Atom – Built to Protect Everything You Value" and the accompanying reservation disclaimer; Ledger, *Ledger Atom™*, https://shop.ledger.com/pages/ledger-atom, FAQ "Can *Ledger Atom™* make phone calls? Is this a phone?" (last visited Oct. 17, 2026).

[37] Jamie Crawley & AI Boost, *Under Pressure, Ledger Unveils Plan to Turn Its Crypto Hardware Wallet into a Smartphone*, CoinDesk (Oct. 15, 2026), https://www.coindesk.com/tech/2026/10/15/under-pressure-ledger-unveils-plan-to-turn-its-crypto-hardware-wallet-into-a-smartphone (reporting Ledger's statements about trade-ins and possible future upgrade promotions).

F. Available designs that prevent sensitive operation after tampering

On information and belief, feasible protective designs available before Baylor's purchases could have prevented, detected, or exposed the alleged compromise while preserving the product's intended function. They included protection of the complete path by which recovery information reaches the display, physical barriers to unauthorized component access, persistent tamper detection, and refusal to generate or expose secrets after an integrity failure.

A secure design must protect confidential recovery information as it is rendered into display data and communicated through the circuitry necessary to present it to the user. Protecting the Secure Element alone does not protect recovery information that an unauthorized component can acquire elsewhere. Reasonable alternatives included protected interconnections, authenticated component relationships where appropriate, tamper-resistant enclosure or encapsulation of the sensitive path, and testing of the complete assembled device against interception during normal setup. On information and belief, additional feasible protections included encrypting sensitive display communications and authenticating receiving components, with protection continuing through the receiving component, and eliminating, isolating, or physically shielding unnecessary accessible test points.

An effective tamper response would prevent a compromised device from generating, displaying, or using recovery information until its secure condition was restored through an appropriate manufacturer-controlled process or the device was replaced. A persistent tamper state could preserve evidence of unauthorized opening or interference during shipment and storage, including while the device lacked external power, and prevent ordinary reset or firmware reinstallation from clearing that condition. The response must operate before the first sensitive initialization of an altered new device, when the user's recovery information has not yet been generated.

Recognized cryptographic-module security frameworks describe progressively stronger physical protections, including tamper evidence, barriers to access, detection, and response. The FIPS 140-3 framework has four security levels; its strongest physical-security category includes an enclosure or protective envelope designed to detect and respond to physical penetration. Those

approaches provide engineering benchmarks for device-appropriate protection of the complete secret-handling path, including prevention of sensitive operation when integrity is lost.[38]

A June 2025 security policy for Senetas CN Series network encryptors describes a tamper circuit that remains active without external power, destroys a protected master key when triggered, records the condition upon restart, and blocks data output in an unactivated state. That existing design illustrates mechanisms for preserving a tamper response across power states and withholding sensitive operation pending secure reconfiguration; adaptation to a consumer hardware wallet requires consideration of its dimensions, power requirements, cost, and intended use.[39]

Protective packaging and enclosure designs were also in commercial use in the hardware-wallet market before Baylor's purchases. In December 2018, Coinkite described uniquely serialized security bags whose identifiers were permanently recorded in the enclosed wallet, together with a welded transparent enclosure intended to make added hardware more apparent. These complementary measures addressed package substitution, prior access, and concealed additions at different stages of delivery and use.[40]

G. Packaging and distribution controls that reveal interference before use

Reasonably secure packaging required more than a closure that could be replaced without an individualized indication of interference. Feasible protective layers included destructible seals or enclosures covering access points, unique package identifiers linked to the particular device, and a manufacturer-provided means for the consumer to verify that association before generating recovery

---

[38] Nat'l Inst. of Standards & Tech., FIPS PUB 140-3, *Security Requirements for Cryptographic Modules* § 3 (Mar. 22, 2019), https://csrc.nist.gov/pubs/fips/140-3/final; Nat'l Inst. of Standards & Tech., *Implementation Guidance for FIPS 140-3*, https://csrc.nist.gov/csrc/media/Projects/cryptographic-module-validation-program/documents/fips%20140-3/FIPS%20140-3%20IG.pdf (mutable document; retrieved edition retained in counsel's source file) (physical-security engineering benchmarks, not a certification requirement alleged to bind Ledger).

[39] Senetas Corp. Ltd., *CN Series Non-Proprietary Security Policy* § 9.3.3, at 64 (ver. 1.02, June 2025), https://csrc.nist.gov/CSRC/media/projects/cryptographic-module-validation-program/documents/security-policies/140sp4869.pdf (tamper-response operation; printed page number, not PDF viewer count).

[40] Coinkite, *Some Other Wallets.fail* (Dec. 28, 2018), https://blog.coinkite.com/other-wallet-fail/.

information. Combining those features with protected hardware and a persistent tamper response would reduce the ability to substitute, open, alter, and reseal a product without detection.

The package and device identifiers could be recorded at manufacture and checked at authorized transfers and first activation, with inconsistent identifiers, duplicate activation, or an unexplained chain-of-custody exception triggering quarantine and verification. Packaging controls also included secure custody of unused seals and containers, separation of returned products from new inventory, inspection of compromised shipments, and investigation of material changes in the businesses handling authorized stock. Those protections must operate at manufacturer-to-distributor and distributor-to-retailer transfers as well as at the final sale; prohibiting retail returns alone does not verify newly supplied inventory.

These measures perform complementary functions. Physical barriers impede access; tamper evidence reveals interference; detection and response prevent sensitive operation; and traceability helps identify substituted or recirculated products. On information and belief, Ledger's use of ordinary closures for Baylor's devices, combined with the alleged hardware and authentication limitations, omitted protections that would have interrupted the compromise before his recovery information was exposed.

Reasonable testing included attempting to open, alter, and reseal an authentic device and its packaging; determining whether an added component could acquire recovery information during prescribed setup; testing whether Genuine Check still succeeded; and determining whether detected interference prevented the device from performing sensitive operations. The tests needed to cover the assembled product, relevant hardware revisions, packaging configurations, new inventory moving through authorized distributors, and foreseeable returns or substitution pathways. Testing also needed to examine concealed additions beneath display assemblies, access through exposed test points, and modifications that preserve the original battery and outward appearance.

Ledger also controlled the communication at the last practical point before exposure. An adequate warning would have explained that the successful check authenticated a component without excluding a concealed implant elsewhere, that apparently intact packaging did not resolve that limitation, and that proceeding could expose newly generated recovery information. It would

have directed the purchaser not to rely on Genuine Check alone while whole-device integrity remained unverified, and to obtain appropriate verification, a verified replacement, or a secure alternative before generating recovery information or funding the affected accounts. Baylor would have heeded that warning.

H. Continuing injury and a protective recall and inspection program

Baylor presently wants to continue using Ledger hardware wallets and to use or obtain a Ledger device whose physical security Ledger can professionally verify or correct. He wants the security characteristics represented for the products he purchased. His decision to quarantine the affected devices does not end that desire. He cannot determine from a successful Genuine Check, apparently intact packaging, or the outward appearance of a device whether its recovery-information path is free from the concealed interference alleged here.

Baylor's knowledge of the earlier compromise does not tell him whether his retained devices can be reliably corrected or whether newly obtained Ledger hardware is free from the same concealed condition. He presently wants to use Ledger hardware with the represented protective characteristics, but cannot make that decision reliably while Ledger's official authentication leaves whole-device physical integrity unresolved. A payment for the completed loss would not require accurate future security communications, provide reliable manufacturer-supported verification, or correct the distribution and initialization practices that created that uncertainty. Those prospective corrections would permit him to evaluate and use Ledger hardware on an informed basis. The same unresolved question affects his ability to rely on Ledger's official seller designation and written assurances when selecting replacement hardware. Correcting the authentication alone would not correct misleading representations about the source and condition of newly delivered products.

Ledger's current buying guidance directs confident consumers toward physical inspection while cautioning them not to damage the device. Its linked hardware-integrity guidance specifically warns that Flex is not designed for routine opening, says internal inspection should ideally be performed by qualified technical personnel, and strongly discourages owner disassembly because it can cause irreversible visible damage and make reassembly highly difficult. Consumers confronting an undetected implant therefore face a software check that cannot resolve the condition and a

physical examination that Ledger warns can damage the product. A reliable remedy requires qualified inspection or verified replacement without requiring consumers to open their own devices, bear the resulting damage, or surrender warranty or statutory rights.[41]

As of October 12, 2026, Ledger's publicly available consumer guide for Germany continued to promote Flex and Stax and state that "a Ledger wallet has never been hacked." That broad assurance does not explain the distinction between an uncompromised Secure Element and an assembled device carrying a concealed physical implant. The continuing presentation reinforces the need for accurate, coordinated security disclosures and reliable verification before sensitive use.[42]

Reliable inspection must address the assembled device and every material path through which recovery information can be displayed, captured, or transmitted. Repeating Genuine Check does not exclude an implant outside the authenticated Secure Element. A comparison to a generic photograph cannot by itself establish the absence of circuitry concealed beneath a display assembly or elsewhere within the device. Ledger controls the original product specifications, authentication design, manufacturing information, and distribution records necessary to develop and validate model-specific examination protocols. Those protocols must address unauthorized components, altered display assemblies, concealed additions, and device-resident alterations capable of exposing recovery information. A written result must identify what was examined, the method used, and whether the examination established physical integrity or left an unresolved condition. An inconclusive examination must not be reported as confirmation that the complete device is secure.

[41] Ledger, *Best Practices to Securely Buy Your Ledger Signer*, https://www.ledger.com/academy/topics/ledgersolutions/best-practices-to-securely-buy-ledger-signer; *see also* Ledger, *Check Hardware Integrity*, Ledger Flex tab, "Important notice," https://support.ledger.com/article/4404382029329-zd (Flex-specific warning reproduced in Plaintiff's "Do not disassemble" screenshot on file with counsel); Ledger Donjon, *Genuineness*, https://donjon.ledger.com/threat-model/device-genuineness/.

[42] Ledger, *Crypto in Germany: The Ultimate Guide*, https://www.ledger.com/academy/topics/country-guides/crypto-in-germany-the-ultimate-guide (Oct. 12, 2026 text cited in the supplied draft; preserve that dated version for the quoted historical statement).

Plaintiff seeks the prompt establishment of a Ledger-funded protective recall and professional inspection program for the Covered Devices held by Class members, regardless of seller or distribution channel. No Class member must disassemble a device or provide an independent technical report as a condition of requesting professional inspection. The program must prevent additional exposure when a Class member resumes use of retained or replacement Ledger hardware. Qualified Ledger hardware-security personnel or independent specialists must examine submitted devices under validated, model-specific protocols addressing the complete recovery-information path. Ledger must pay the necessary intake, shipping, examination, and secure-return costs. The protocol must account for Ledger's own warning that opening a Flex can irreversibly damage it, and must not condition eligibility on the owner performing that disassembly. Where examination identifies compromise, reliable verification cannot promptly be completed, or examination damages the device, the program must provide a new, professionally verified replacement through secure and traceable delivery before the consumer resumes sensitive use. Ledger must correct the relevant security deficiency before presenting a replacement as safe for that use.

The program's scope must follow the challenged security condition and the available technical and traceability evidence. Reports involving different Ledger models and sales channels, including the reported Flex implant, support protection beyond CryptoBilis. An intact Secure Element, apparently unopened packaging, or a different seller does not resolve whether concealed hardware can acquire recovery information. The requested program therefore includes the Covered Devices held by Class members across manufacturing and assembly facilities, production lots, and distribution channels. Any proposed exclusion must be supported by reliable component, manufacturing, custody, and examination evidence sufficient for the Court to determine that the excluded devices do not require the protective measure at issue. Ledger must provide that information for independent assessment and the Court's determination of appropriate scope.

The program must provide secure intake, documented custody, written inspection results, independent technical oversight, and preservation of suspect components before destructive examination or reset. Participation must not require a release of claims or forfeiture of warranty or

statutory rights. Neither Ledger nor an examiner may obtain the owner's recovery phrase, private keys, PIN, control of assets, or unnecessary wallet or account identifiers. Where recovery information may have been exposed, the program must provide secure instructions and assistance enabling the owner to generate fresh recovery information on trusted hardware and migrate assets under the owner's exclusive control. A replacement device must not be presented as correcting exposure if the owner continues using compromised recovery information.[43]

The same prospective protection requires Ledger to identify and quarantine unverified inventory within its control, implement validated physical-integrity and traceability controls before further distribution, correct its authentication and setup communications, and give affected consumers direct and prominent notice of available verification and protective measures. Corrective notices must reach consumers where Ledger directs purchasing and use, including the official reseller directory, purchasing links, activation instructions, the official application, and support communications. Removing a seller from a directory does not notify every prior purchaser or determine whether devices already delivered through that or another channel contain an implant. Plaintiff seeks court-supervised implementation with defined completion milestones and independent technical reporting. This relief addresses the continuing inability to evaluate and use Ledger hardware with the represented security protections and the risk of future exposure during sensitive use. The announced regional sales suspensions, sample inspections, and backroom-stock requirements do not determine the condition of each product already delivered to a consumer. They cannot substitute for direct notice and reliable verification of those products. The requested relief addresses that unresolved need, with model-specific inspection and replacement standards supported by the technical evidence. Those corrections must separately address what Ledger's official reseller designation, partner vetting, sourcing requirements, and product-integrity

[43] Ledger, What to Do If Your Crypto Project Gets Hacked, https://www.ledger.com/academy/basic-basics/launch-a-crypto-project-securely/what-to-do-if-your-crypto-project-gets-hacked (background for owner-controlled protective measures; the requested program is Plaintiff's proposed relief).

assurances do and do not establish about an individual unit. Ledger must not present commercial authorization alone as verified absence of physical tampering.

Contemporaneously with filing, Plaintiff will provide the separate notice and corrective demand required by Civil Code section 1782. Plaintiff presently seeks injunctive relief under the CLRA and UCL. CLRA damages, monetary restitution, and other relief subject to the statutory notice and correction requirements are reserved for amendment after compliance with section 1782.

V. CLASS ACTION ALLEGATIONS

Plaintiff brings every cause of action in this Complaint on behalf of himself and the same Class under Federal Rule of Civil Procedure 23(a) and (b)(3), and seeks certification of appropriate common injunctive relief for that Class under Rule 23(b)(2). Plaintiff proposes one Class, defined as follows:

> All natural persons who purchased a Ledger hardware wallet primarily for personal, family, or household use and, before class certification, suffered an unauthorized loss of cryptocurrency through spyware installed in that wallet before delivery to them.

For purposes of this Complaint, "spyware" means an unauthorized hardware implant, component substitution, or device-resident alteration capable of acquiring or transmitting recovery information without the user's authorization. "Covered Devices" means Ledger hardware wallets implicated by that mechanism, including Flex, Nano X, Stax, and other Ledger models. The Class is not limited to CryptoBilis, an authorized seller, a particular model, or a particular country of purchase or residence. A loss caused only by phishing, voluntary disclosure of recovery information, or malware unrelated to spyware in the delivered hardware is outside this definition.

Class membership turns on the purchase, the pre-delivery spyware, and the resulting unauthorized cryptocurrency loss—not on a determination that Ledger is liable. Ledger's product, distribution, support, incident, and examination records, together with purchase, device, and transaction evidence, can identify members. Recovery remains subject to proof of the elements and timeliness of each claim, without separate purchaser, theft, model, seller, or injunctive classes.

Excluded from the Class are Ledger and its officers and directors; persons who participated in installing or knowingly distributing the spyware or carrying out the unauthorized transfers;

entities controlled by Ledger; the assigned judicial officers and their immediate families; and persons who timely and validly request exclusion from a class certified under Rule 23(b)(3).

Numerosity. On information and belief, the Class is sufficiently numerous that joinder is impracticable. The reported spyware incidents across multiple models and distribution channels, Ledger's investigation and customer contacts, and the concealed nature of the alleged compromise support the need for aggregate treatment. The number and identities of qualifying victims will be determined from incident, support, sales, distribution, device-examination, and transaction records; Ledger's total sales are not treated as a count of spyware victims.

Commonality. Common questions include whether Ledger adequately protected the recovery-information path against pre-delivery spyware; whether Genuine Check and the associated communications disclosed that an authentic chip could coexist with an implant; what Ledger knew and when; whether its design, packaging, testing, and distribution controls reasonably addressed the risk; whether its product-security affirmations and omissions were misleading; and what corrective measures are necessary. The design, warranty, negligence, and consumer-protection claims arise from that shared manufacturer-level conduct.

Typicality and adequacy. Baylor purchased two Flex devices for personal use, followed Ledger's purchasing and setup directions, received successful Genuine Check results, and suffered the alleged spyware-related theft of his cryptocurrency. His claims present the same distinction between an authentic Secure Element and the integrity of the complete product. He seeks recovery for the same type of property loss and correction of the practices that prevent reliable future use. He will fairly and adequately protect the Class and has retained counsel experienced in complex and class litigation.

Predominance and superiority. Ledger's design specifications, authentication, standardized communications, knowledge, and distribution controls are susceptible to common documentary and technical proof. Individual ownership, device configuration, transaction history, causation, and loss amounts can be evaluated through a common evidentiary process without repeatedly litigating the manufacturer-level issues. Class treatment avoids duplicative expert examinations and adjudications

and provides a practical means of pursuing claims whose investigation and litigation costs would otherwise deter recovery.

Damages. Plaintiff and the Class seek the legally recoverable value of cryptocurrency lost through the alleged spyware compromise, together with recoverable product-value loss and incidental and consequential expenses under the applicable counts. A damages method consistent with the liability theory will account for device and transaction records, valuation, refunds, recoveries, and any other offsets, without double recovery. The difference in the amounts lost does not change the alleged common mechanism.

Prospective relief. Ledger's continuing authentication, warning, distribution, and verification practices are common to the Class. Baylor retains the affected hardware and presently wants to use or obtain reliably verified Ledger devices. He seeks a uniform corrective program that gives Class members reliable information, professional examination, and verified replacement where needed before further sensitive use. Certification under Rule 23(b)(2) is requested only insofar as the evidence establishes indivisible prospective relief appropriate to the Class as a whole; monetary awards are sought under Rule 23(b)(3).

Case management. Plaintiff seeks certification of this single Class for all six counts. If particular issues require separate adjudication, Rule 23(c)(4) permits common issues to be resolved for the same Class, with individualized determinations where necessary. Model-specific technical protocols and transaction records can address factual differences without creating separately defined classes. Plaintiff may refine the definition in light of discovery and the Court's orders.

VI. CAUSES OF ACTION

FIRST CAUSE OF ACTION
BREACH OF EXPRESS WARRANTY
California Commercial Code §§ 2313, 2714, and 2715
Plaintiff and the Class against Ledger SAS

Plaintiff incorporates the allegations in Sections I through V. Plaintiff brings this count on behalf of himself and the Class.

Ledger made express affirmations of fact and descriptions of the goods through two distinct communications. First, its official reseller designation, in the purchasing and security context alleged above, described goods supplied through a manufacturer-selected channel as protected by Ledger's product-integrity and distribution safeguards and suitable for secure initialization. The channel protections Ledger describes in its own publications corroborate that asserted meaning. Those factual product descriptions create express warranties under California Commercial Code § 2313(1)(a)–(b) to the extent they formed part of the basis of the bargain. Second, Ledger's successful Genuine Check, furnished with the hardware and prescribed initial setup, communicated in context that the particular delivered device was suitable to proceed safely through Ledger's initialization. The warranties concern the described physical condition and security functionality, not merely the authenticity of one chip.

Ledger supplied its official directory to guide the purchasing decision and its authentication to guide initial use. Baylor followed that directory, relied on Ledger's designation of CryptoBilis in selecting his source, and purchased the two Flex devices as new products of Ledger's authorized channel. The product-integrity description conveyed by that designation in the security context alleged above formed part of the basis of his bargain. The manufacturer-prescribed authentication was included product performance and separately reinforced his decision to proceed with setup and commit cryptocurrency. These are cumulative assurances concerning the goods and their initial protective function.

The channel-integrity warranties are asserted against Ledger for Ledger's own descriptions and representations concerning its goods and their distribution safeguards. They do not depend on attributing every independent statement or act of the reseller to Ledger. Nor does the use of the word "recommends," rather than "warrants" or "guarantees," defeat an otherwise actionable factual affirmation or description under California Commercial Code § 2313(2). The physical condition represented for products supplied through the designated channel is independently capable of proof or disproof.

On information and belief, one or more of Baylor's devices contained the concealed physical alteration described above when delivered. Such a device did not conform to the physical-integrity

and secure-initialization condition conveyed by the official purchasing designation in context, even if its original Secure Element remained genuine. On information and belief, the delivered goods and included security functionality also failed to conform to the setup-stage affirmation: inadequate protection of the recovery-information path, ineffective indications of prior interference, and the absence of an effective tamper response allowed the altered device to pass the supplied authentication and expose newly generated recovery information. The inadequate disclosure left that material condition unresolved. A technically successful check of an authentic component does not establish conformity of the complete product with the alleged warranties.

Plaintiff paid for the products, used Ledger's official setup and authentication, generated recovery information on the devices, and kept that information offline.

Before filing, Baylor reported the unauthorized losses to Ledger, which acknowledged his report and sought device, purchase, delivery, and setup information in its October 12, 2026 response in support case 00285187. Contemporaneously with filing this Complaint, Plaintiff will also provide Ledger with written notice identifying the alleged breaches and security deficiencies and demanding corrective relief. That notice identifies the product-integrity meaning conveyed by Ledger's official reseller designation, Ledger's published descriptions of reseller selection, sourcing protections and restrictions on returned goods, the alleged delivery of altered goods through that channel, and the separate setup-stage warranty breach.

The breach was a substantial factor in Plaintiff's loss. Ledger's purchasing designation induced him to obtain the devices through its authorized channel; the delivered products' nonconformity exposed recovery information; and the successful setup result induced him to commit assets. He would not have obtained and funded hardware through that channel had the actual compromised condition or material limitation been adequately disclosed. Loss of cryptocurrency through exposure of recovery information was foreseeable to Ledger, which supplied the product and authentication for the specific purpose of securing access to that property.

Plaintiff seeks direct, incidental, and consequential relief under California Commercial Code sections 2714 and 2715 for breach of Ledger's public product affirmations and descriptions. Replacing the hardware after exposure cannot restore the secrecy of the compromised recovery

information or return cryptocurrency already transferred. Plaintiff does not concede any agreed disclaimer or limited remedy. If Ledger establishes an otherwise applicable limitation, Plaintiff challenges it, as appropriate, under sections 2316(1) and 2719, including inconsistency with an express warranty or failure of an exclusive remedy's essential purpose.

Plaintiff and the Class seek the difference between the value of the goods and included security functionality as represented and as delivered, together with recoverable incidental and consequential damages under California Commercial Code §§ 2714 and 2715. Consequential damages include the value of cryptocurrency lost through the alleged spyware compromise and reasonable response and recovery expenses to the extent incurred and proven. Plaintiff's cryptocurrency loss exceeds $1 million. No duplicate recovery is sought.

SECOND CAUSE OF ACTION
VIOLATION OF THE CONSUMERS LEGAL REMEDIES ACT
(INJUNCTIVE RELIEF ONLY)
California Civil Code § 1750 *et seq.*
Plaintiff and the Class against Ledger SAS

Plaintiff incorporates the allegations in Sections I through V. Plaintiff brings this count on behalf of himself and the Class and seeks present injunctive relief to prevent continuing deceptive practices and future exposure during use of the Covered Devices. CLRA damages, monetary restitution, and other relief subject to the notice and correction requirements of Civil Code section 1782 are reserved for amendment after compliance with that statute.

Plaintiff and the Class are consumers under Civil Code § 1761(d). The Covered Devices are tangible consumer goods under § 1761(a), purchased primarily for personal, family, or household use. Ledger is a person under § 1761(c). The transactions included the manufacturer-supplied security functionality, packaging, initial setup, and authentication associated with those goods.

Ledger represented security characteristics and benefits the goods did not possess, in violation of Civil Code § 1770(a)(5), and a standard or quality the goods did not meet, in violation of § 1770(a)(7). Ledger's purchasing representation concerned product integrity and suitability for secure initialization conveyed by Ledger's manufacturer-controlled designation of the purchasing channel. Ledger's own descriptions of reseller selection, sourcing safeguards, and restrictions on

returned goods corroborate the asserted meaning of that designation. An altered device does not possess the alleged physical-integrity condition merely because its Secure Element is authentic. Separately, the successful Genuine Check and prescribed setup communicated a condition for secure initial use without adequately disclosing that the result could coexist with physical interception of recovery information.

Ledger's successful result and setup directions communicated only part of the material security condition. Ledger knew the scope of the authentication it designed and the difference between an authentic component and an uncompromised complete device. Having furnished that result to guide initial use, Ledger was required to disclose the material limitation that a concealed component could acquire recovery information while remaining undetected. The condition concerned the wallet's central protective function and rendered the communicated characteristics, benefits, standard, and quality misleading. Having directed consumers to a manufacturer-selected purchasing channel as a product-integrity safeguard, Ledger also had to disclose facts necessary to prevent that direction from misleading purchasers about the concealed physical-interception risk. The omission concerned the delivered goods despite the official seller designation and subsequent successful component check.

The challenged communication was made by Ledger through its official application during Plaintiff's initial setup of the two Flex devices purchased on July 13 and September 4, 2026. It identified the devices as 'Genuine' and allowed Plaintiff to proceed. Plaintiff received that result before generating recovery information and committing assets. The material omitted information was the physical-implant limitation described in the factual allegations above. Ledger also made the purchasing representation through its own Official Reseller Network when Baylor selected CryptoBilis for the July 13 and September 4 purchases. Baylor relied on that official designation in choosing the source of his new Flex devices. The challenged purchasing representation is the product-integrity meaning conveyed by that designation in the security context alleged above, not a statement made solely by CryptoBilis.

The condition and omission were material. A reasonable consumer buying a hardware wallet to safeguard recovery information would consider whether the manufacturer's successful check

addresses an alteration capable of capturing that information. Plaintiff actually relied on Ledger's official purchasing designation in choosing his source and on the later successful result in deciding to proceed with sensitive setup and funding. An adequate warning would have caused him to withhold assets from the affected recovery information and obtain a secure alternative.

Plaintiff's reliance during setup caused him to expose his assets to the affected recovery information and resulted in the theft losses alleged above. He also received security functionality worth less than represented because it failed to address the concealed condition central to its protective purpose. Those completed injuries establish his stake in the challenged conduct. His present desire to use or obtain Ledger hardware with verified or corrected physical security, and inability to rely on the challenged authentication for that purpose, supply the prospective injury for which he seeks an injunction. A later damages award for the completed loss would not stop the continuing deception or permit informed future use. Reliable future purchasing requires correction of the authorized-channel product-integrity representations as well as the authentication and setup disclosures.

Plaintiff seeks only prospective injunctive relief under the CLRA in this initial Complaint. Contemporaneously with commencement of this action, Plaintiff will provide Ledger with a separate written notice identifying the particular violations alleged here, including the authorized-channel product-integrity and setup representations, and demanding corrective relief under Civil Code section 1782(a), including the inspection and replacement program described above. After at least 30 days have elapsed following commencement of this action and the applicable statutory notice and correction periods have expired, Plaintiff intends to amend under section 1782(d) and Federal Rule of Civil Procedure 15 to seek available CLRA damages and other remedies, subject to sections 1782(b) and (c).

Plaintiff seeks preliminary and permanent injunctive relief under Civil Code section 1780(a)(2) correcting Ledger's continuing deceptive authentication, disclosure, distribution, and initialization practices. Ledger must correct misleading representations about the integrity of goods purchased through its official network and the scope and implementation of reseller vetting and sourcing standards. It must also provide accurate security representations, prominent disclosure of

unresolved physical-interception risks before sensitive use, and reliable standards for physical-integrity verification. It must not present component authentication or an inconclusive physical examination as assurance that the complete device is uncompromised. The immediate protective recall, professional inspection, and secure-replacement program is also requested under Count VI. Plaintiff seeks reasonable attorney's fees and costs under section 1780(e). This count requests no damages or monetary restitution at this time. The statutory protections and remedies may not be waived contrary to section 1751.

THIRD CAUSE OF ACTION
NEGLIGENCE
Plaintiff and the Class against Ledger SAS

Plaintiff incorporates the allegations in Sections I through V. Plaintiff brings this count on behalf of himself and the Class.

As the designer and manufacturer of a security product intended to protect access to separately owned assets, Ledger owed foreseeable users reasonable care in designing, manufacturing, packaging, testing, and validating the hardware's recovery-information protections and in supplying accurate instructions and authentication. Ledger also owed reasonable care in the distribution-security functions it undertook and controlled. The duty encompasses foreseeable interference with a security device before the consumer receives and initializes it, including access during manufacturing, assembly, storage, shipment, retail custody, and returns handling.

Ledger also undertook to provide purchasers with an initial security assessment through its official application and Genuine Check, specify the initial-use procedure, and identify its official distribution channel. Ledger knew that purchasers would use those functions to decide whether to generate recovery information and commit cryptocurrency. Having supplied the assessment and directed that reliance, Ledger owed reasonable care in performing the functions it undertook and communicating the material limits of the result at the point where it invited the purchaser to proceed. That duty required an accurate explanation before generation of recovery information, when the foreseeable exposure could still be prevented. Baylor relied on that assessment and procedure before exposing his assets.

Ledger knew or should have known that users would rely on its authentication in deciding whether to generate recovery information and commit cryptocurrency; that exposure of that information could give an attacker control of the assets; and that pre-delivery interference with a security device was a foreseeable hazard. The magnitude of loss could be substantial even for a single consumer.

Ledger breached its duties by inadequately protecting the complete recovery-information path; failing reasonably to test authentic devices against opening, alteration, and resealing; failing to provide effective tamper detection and a response that prevented sensitive operation; using inadequate packaging and verification controls; and communicating a successful result without adequate disclosure of the unresolved condition. On information and belief, it also failed reasonably to implement and enforce inventory, returns, revalidation, and incident-response controls associated with its official distribution channel. The alleged breach also includes failure to provide adequate transaction-stage and pre-initialization warnings in response to the physical-implant information received before Baylor's purchases and loss.

Those failures were substantial factors in Plaintiff's harm. The deficient protections permitted an altered device to reach him without effective indication of interference, and the absence of an effective tamper response allowed exposure of new recovery information. Ledger's successful security assessment and inadequate disclosure induced him to proceed and commit assets. Reasonable performance of the undertaken functions and effective protective layers would have interrupted that sequence. On information and belief, the same failures permitted pre-delivery spyware to acquire Class members' recovery information and were substantial factors in their unauthorized cryptocurrency losses.

The malicious actors' acquisition and exploitation of recovery information were foreseeable manifestations of the risk against which the product and authentication were supplied. Their intervention does not eliminate the causal role of the alleged product and warning deficiencies.

Plaintiff and the Class lost cryptocurrency they owned independently of the hardware wallets and their software. They seek compensation for that separate property and other legally recoverable

consequential harm according to proof. This tort claim is pleaded in the alternative to the warranty claim, without duplicate recovery.

FOURTH CAUSE OF ACTION
STRICT PRODUCTS LIABILITY - DESIGN DEFECT
Plaintiff and the Class against Ledger SAS

Plaintiff incorporates the allegations in Sections I through V. Plaintiff brings this count on behalf of himself and the Class.

Ledger designed, manufactured, and placed the Covered Devices and their packaging into the stream of commerce for ultimate purchasers to generate and protect recovery information and control their cryptocurrency. Ledger intended consumers to initialize them through the official process without first performing a forensic examination of internal components.

On information and belief, the original design inadequately protected the recovery-information path against foreseeable physical interference and allowed a delivered device to proceed with sensitive initialization despite an undetected alteration. The challenged design includes the enclosure and component protections, detection of and response to tampering, the packaging's failure to reveal prior interference, and the relationship of those safeguards to Genuine Check. Those choices permitted the alleged compromise to defeat the product's security purpose.

The challenged design choices existed when Ledger placed the products into distribution. Their inadequacy made the recovery-information path susceptible to foreseeable pre-delivery interference and allowed an altered device to proceed through Ledger's successful initial check. The original defect was Ledger's failure to protect, detect, or stop that exposure through the hardware and security process it supplied. That defect accompanied the product through the supply chain and operated when Baylor followed the prescribed setup. The identity and location of the person exploiting the defect do not remove its substantial causal role in the resulting exposure.

The risks of the challenged design outweighed its benefits. The gravity of exposing recovery information and the associated assets, the known prospect of pre-delivery tampering, and the product's security purpose outweighed the benefits of the inadequate protective choices. Feasible alternatives included the physical barriers, persistent tamper detection and response, protected

information paths, and verifiable packaging alleged above. They would have reduced the risk before initialization and funding while preserving the product's useful function.

Alternatively, the product failed to perform as safely as an ordinary consumer would expect during intended and reasonably foreseeable use. A consumer who obtains a device sold as new, follows the prescribed setup, receives the manufacturer's successful check, and generates recovery information on the device reasonably expects that the process will not expose that information to a concealed unauthorized component. Baylor followed that process, yet the alleged original security deficiencies allowed the information controlling his assets to be acquired.

Plaintiff used the Flex in an intended and reasonably foreseeable manner by following official setup, generating recovery information on the device, and committing cryptocurrency after a successful check. Attempts by criminals to modify hardware wallets before delivery were a foreseeable product risk of the kind described above.

On information and belief, the original defect was a substantial factor in the interception of recovery information and the resulting unauthorized transfers. Plaintiff and members of the Class suffered loss of separately owned cryptocurrency. They seek compensatory damages according to proof, in the alternative to other available theories and without duplication.

FIFTH CAUSE OF ACTION
STRICT PRODUCTS LIABILITY - FAILURE TO WARN
Plaintiff and the Class against Ledger SAS

Plaintiff incorporates the allegations in Sections I through V. Plaintiff brings this count on behalf of himself and the Class.

Ledger manufactured and distributed the Covered Devices with their packaging, setup, and authentication. On information and belief, the risk that unauthorized pre-delivery interference could expose recovery information despite successful Secure Element authentication was known or knowable in light of the generally recognized scientific and technical knowledge available when the relevant devices were manufactured and distributed. Ledger's knowledge included the scope of its own design and the supply-chain research and implant information available at the relevant time. The reported March 4, 2026 disclosure and the earlier research described above

concern notice of the relevant attack mechanism before Baylor's purchases, not advance identification of his particular units.

That risk presented a substantial danger to users' separately owned cryptocurrency during intended initial use. It was concealed within the product and was not a condition an ordinary purchaser could identify from the unopened retail packaging, an apparently normal device, or a successful result from the manufacturer's own check.

Ledger failed to provide an adequate warning before sensitive initialization that a successful Genuine Check did not exclude an unauthorized component elsewhere in the device; that apparently intact packaging did not resolve that limitation; and that the condition could expose newly generated recovery information. An adequate warning would have explained the specific limitation and directed the purchaser not to rely on Genuine Check alone while whole-device integrity remained unverified, and to obtain appropriate verification, a verified replacement, or a secure alternative before generating recovery information or committing assets.

Plaintiff did not receive an adequate warning of that risk before proceeding. He would have heeded one by withholding assets pending a secure alternative. The failure to warn was therefore a substantial factor in his exposure to the alleged compromise and ensuing loss. On information and belief, the same failure to provide an adequate warning before sensitive use contributed to Class members' spyware-related losses. Plaintiff and the Class seek compensatory damages for their separately owned cryptocurrency and other recoverable harm according to proof.

SIXTH CAUSE OF ACTION
VIOLATION OF THE UNFAIR COMPETITION LAW
(INJUNCTIVE RELIEF ONLY)
California Business and Professions Code § 17200 *et seq.*
Plaintiff and the Class against Ledger SAS

Plaintiff incorporates the allegations in Sections I through V. Plaintiff brings this count on behalf of himself and the Class.

Ledger's design, distribution, marketing, authentication, and support of the Covered Devices are business acts and practices within California Business and Professions Code section 17200. Ledger directs those practices to California consumers through the California commerce and

continuing customer relationships alleged above. Those practices include Ledger's own written representations about the physical integrity of products obtained from its official network, its vetting and standards for designated sellers, and the source and custody protections accompanying the goods.

Those practices are unlawful because Ledger misrepresents and omits material security characteristics, benefits, and quality in violation of Civil Code sections 1770(a)(5) and (7). Ledger supplies an initial security determination that permits sensitive setup while withholding the material fact that concealed hardware can acquire newly generated recovery information despite the successful result. For authorized-network purchasers, the unlawful practices also include the product-integrity, vetting, sourcing, and quality representations and related material omissions pleaded under the same CLRA subsections.

Those practices are unfair because they expose consumers to concealed interference with the very secrets the products are purchased to protect while denying consumers a reliable means of determining whether the delivered hardware is compromised. The substantial injury cannot reasonably be avoided by following Ledger's prescribed setup and is not outweighed by countervailing benefits to consumers or competition. Consumers cannot resolve the hidden condition through component authentication, ordinary packaging inspection, or disassembly that Ledger itself strongly discourages because of the risk of irreversible damage. Accurate disclosures, validated integrity verification, effective tamper controls, and secure distribution practices provide feasible means of reducing the injury. The practices also offend the consumer-protection policies embodied in the CLRA. Directing consumers to the official network as a means of safeguarding the integrity of delivered products, while leaving an undisclosed material gap between seller authorization and individual-device integrity, prevents purchasers from avoiding the very risk the direction purports to address.

Those practices are fraudulent because they are likely to deceive reasonable consumers about the condition of newly received hardware and the protection afforded by Ledger's successful authentication. The misleading impression arises from Ledger's official reseller designation, the product's security purpose, the prescribed setup sequence, and the successful result communicated

before the user generates recovery information and commits assets. Ledger knows the material difference between authenticating the Secure Element and excluding an unauthorized component elsewhere in the device. The additional purchasing representation conveys in context that Ledger's designated network supplies new hardware protected by the manufacturer-described distribution safeguards and suitable for secure initialization. Ledger's own purchasing and setup communications are challenged; a third party's unauthorized alteration does not resolve whether Ledger's representations and material omissions were misleading.

Baylor suffered injury in fact and lost money and property as a result. He relied on Ledger's official distribution designation and successful authentication, followed the prescribed setup, and placed his separately owned cryptocurrency under the control of the recovery information generated on the devices. The concealed compromise and misleading security determination caused the unauthorized losses alleged above. Adequate disclosure before sensitive use would have caused him to withhold his assets pending a secure alternative. His expenditure on the devices followed Ledger's official-channel representation, and the later asset commitment followed its authentication. On information and belief, the goods he received did not have the physical-integrity condition and protective functionality conveyed by those representations in context. The two stages of reliance are alleged as parts of the causal sequence, not as duplicate losses.

Baylor retains the quarantined devices and presently wants to use or obtain Ledger hardware whose physical security has been reliably verified or corrected. Ledger's continuing practices prevent him from determining whether retained or newly obtained hardware can be trusted for that use. Compensation for the completed loss cannot require Ledger to disclose the limits of its ongoing authentication, provide the manufacturer-controlled information needed for reliable verification, or correct its continuing distribution and initialization practices. Purchasing another device without those corrections leaves the same concealed integrity question unresolved. Ledger's own instruction to Baylor to use a new recovery phrase without using the current device underscores the need for a reliably verified or corrected product on which he can securely resume the intended use. An announcement of additional protections for an unreleased product does not establish the integrity of

his retained Flex devices or supply a present means of safely using them. Legal damages therefore do not provide an adequate remedy for the prospective injury alleged here.

Plaintiff seeks preliminary and permanent injunctive relief under section 17203 requiring accurate security communications, correction of misleading authorized-network product-integrity, vetting, and sourcing representations, validated physical-integrity verification, and the protective recall, professional inspection, and secure-replacement program alleged above, together with effective controls against further distribution and sensitive initialization of compromised products. The program addresses future use and exposure of recovery information through model-specific protocols and the Court's determination of appropriate scope. Plaintiff requests no damages, restitution, disgorgement, or cash reimbursement under this count. Plaintiff seeks reasonable attorney's fees and costs under Code of Civil Procedure section 1021.5 and other applicable law.

VII. PRAYER FOR RELIEF

WHEREFORE, Plaintiff requests judgment against Ledger SAS as follows:

A. Certifying the Class under Federal Rule of Civil Procedure 23(b)(3) and, for appropriate common prospective relief, Rule 23(b)(2), or certifying particular common issues for that same Class under Rule 23(c)(4); appointing Kenneth Baylor as Class representative; and appointing his counsel as Class counsel;

B. Awarding Plaintiff and the Class damages under Count I according to proof, including recoverable product-value loss and incidental and consequential damages;

C. Awarding Plaintiff and the Class the legally recoverable value of cryptocurrency lost under Counts I, III, IV, and V, with Plaintiff's contemporaneous estimate of his loss being approximately $1.05 million, together with proven, recoverable response and recovery expenses, without duplicate recovery;

D. Awarding reasonable attorney's fees and costs under California Civil Code § 1780(e), California Code of Civil Procedure § 1021.5, and other applicable authority;

E. Awarding prejudgment and postjudgment interest as permitted by law;

F. Awarding preliminary and permanent injunctive relief under Counts II and VI for Plaintiff and the Class, to the extent supported by prospective injury and the requirements for the relief

sought, requiring Ledger to cease misleading representations concerning authorized-network product integrity, reseller vetting, sourcing standards, and security verification; accurately describe the controls actually applied to the products and their distribution; and disclose material physical-integrity and Genuine Check limitations before purchase and sensitive initialization, and requiring the immediate protective recall, professional inspection, and secure-replacement program under Count VI. The order should require direct notice to eligible consumers and coordinated corrections in Ledger's reseller directory, purchasing links, activation materials, application, and support communications; Ledger-funded examination of Covered Devices held by Class members under validated, model-specific protocols that account for the risk of inspection damage and do not require owner disassembly; secure intake and documented custody; written findings and independent technical oversight; verified replacement before further sensitive use where a device is compromised, prompt reliable verification is unavailable or inconclusive, or examination damages it; secure instructions and assistance for owner-controlled recovery-information regeneration and asset migration; quarantine and verification of unverified inventory before further distribution; effective manufacturing, packaging, custody, and returns controls; access to the corrective program without purchasing a new premium model or awaiting the release of Ledger Atom; and defined implementation milestones and compliance reporting; and

G. Granting such other relief as the Court determines is just and proper, without duplicate recovery. CLRA damages, monetary restitution, and other remedies subject to Civil Code section 1782 remain reserved pending compliance with that statute. Count VI seeks injunctive relief and associated fees and costs only.

VIII. DEMAND FOR JURY TRIAL

Pursuant to Federal Rule of Civil Procedure 38, Plaintiff demands a trial by jury on all issues so triable.

DATED: October 30, 2026

FROST LLP

By: 

CHRISTOPHER FROST
KEVIN S. DICKER
Attorneys for Kenneth Baylor