Todd M. Schneider (SBN 158253)
Jason H. Kim (SBN 220279)
Matthew S. Weiler (SBN 236052)
Kyle G. Bates (SBN 299114)
SCHNEIDER WALLACE
COTTRELL KONECKY LLP
2000 Powell Street, Suite 1400
Emeryville, California 94608
Telephone: (415) 421-7100
Email: tschneider@schneiderwallace.com
Email: jkim@schneiderwallace.com
Email: mweiler@schneiderwallace.com
Email: kbates@schneiderwallace.com

Kyle W. Roche (*pro hac vice application forthcoming*)
Richard Cipolla (*pro hac vice application forthcoming*)
Jolie Huang (*pro hac vice application forthcoming*)
ROCHE FREEDMAN LLP
99 Park Avenue, 19th Floor
New York, NY 10016
Telephone: (646) 970-7509
Email: kyle@rcfllp.com
Email: rcipolla@rcfllp.com
Email: jhuang@rcfllp.com

Velvel Freedman (*pro hac vice application forthcoming*)
Constantine P. Economides (*pro hac vice application forthcoming*)
ROCHE FREEDMAN LLP
200 South Biscayne Boulevard
Miami, FL 33131
Telephone: (305) 971-5943
Email: vel@rcfllp.com
Email: ceconomides@rcfllp.com

Counsel for Plaintiffs

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA

JOHN CHU and EDWARD BATON, Individually and on Behalf of All Others Similarly Situated,

Plaintiffs,

v.

LEDGER SAS, LEDGER TECHNOLOGIES INC., SHOPIFY (USA) INC., and SHOPIFY INC.,

Defendants.

No. _____

COMPLAINT

CLASS ACTION

DEMAND FOR JURY TRIAL

Individually and on behalf of all others similarly situated, Plaintiffs John Chu ("Chu") and Edward Baton ("Baton"), (collectively, "Plaintiffs"), bring this Action against Defendants Ledger SAS and Ledger Technologies Inc. ("Ledger Technologies"), (collectively, "Ledger") and Defendants Shopify Inc., and Shopify (USA) Inc. ("collectively, "Shopify"). Plaintiffs' allegations are based upon personal knowledge as to themselves and their own acts, and upon information and belief as to all other matters based on the investigation conducted by and through Plaintiffs' attorneys. Plaintiffs believe that substantial additional evidentiary support will exist for the allegations set forth herein, after a reasonable opportunity for discovery.

I. INTRODUCTION

"*We know security means never standing still.*"

-Ledger.

1. Plaintiffs seek redress for the substantial, Class-wide damages that Ledger's and Shopify's misconduct caused in connection with a massive 2020 data breach that those companies negligently allowed, recklessly ignored, and then intentionally sought to cover up.

2. With Shopify assisting as its e-commerce vendor, Ledger purports to provide "the highest level of security for crypto assets." Its primary products are hardware wallets ("Ledger wallets") that store the "private keys" of an individual's crypto-assets. These private keys are akin to a bank-account password in that access to the private keys allows an individual to transfer one's crypto-assets. But unlike a bank-account transaction, crypto-asset transactions are non-reversible: whoever gains access to the private keys associated with a crypto-asset can then transfer or spend that asset with impunity. Ledger purports to provide owners of crypto-assets with the best security to protect private keys from hackers and other bad actors.

3. Ledger thus knows that anonymity is necessary to protect against hacking attempts. Crypto-asset transactions are publicly visible on the underlying blockchain, but nefarious actors cannot identify the owner of particular crypto-assets based solely on public information. Without personally identifying information, hackers face an immense obstacle to targeting an individual's crypto-assets. Conversely, when a hacker knows the identity of a crypto-asset owner, the hacker can construct a workable attack catered to a target.

4. Consequently, to the world of hackers**,** Ledger's customer list is gold. It is a list of people who have converted substantial wealth into anonymized crypto-assets that are transferrable without a trace. Using that list, hackers can manipulate or compel those owners to make untraceable and irreversible transfers of the crypto-assets into the hackers' accounts. The stakes of security for crypto-assets are thus enormous. With anonymity, owning a Ledger wallet is a cutting-edge method of securing crypto-assets. But without anonymity, owning a Ledger device simply creates a target for attackers.

5. Ledger understands these realities and purports to account for them. As Ledger claims in its advertising: "If you don't want to get hacked, get a Ledger wallet." Over the past year, however, Ledger repeatedly and profoundly failed to protect its customers' identities, causing targeted attacks on thousands of its customers' crypto-assets and causing Class members to receive far less security than they thought they purchased when they purchased a Ledger wallet.

6. In mid-2020, between April and June, hackers found and exploited a database vulnerability at Ledger and its e-commerce vendor, Shopify, to obtain a list of Ledger's customers, as well as email addresses and other contact information. By June 2020, Ledger's customer list had made its way onto the internet's black market, making Ledger wallet owners vulnerable.

7. The circumstances grew much worse over the next six months. From June 2020 through December 2020, at least one of the hackers who had acquired the data published it online, providing over 270,000 names, physical addresses, phone numbers, and order information to every hacker in the world. As a direct result, the attacks on Ledger's customers grew exponentially, with customers losing money, facing threats of physical violence, and even feeling vulnerable in their own homes. Indeed, using the customer shipping addresses that Ledger and Shopify had failed to protect, hackers threatened to enter the homes of and attack Ledger customers unless those customers made untraceable ransom payments.

8. In the face of these obviously emergent circumstances, rather than acting to protect its customers, Ledger stood still. It did not even inform its customers of the breach. Instead, it initially denied that any breach had occurred and continued to claim its products provided the best

possible protection for crypto-assets. As the customer list began to spread on the dark web, Ledger admitted the existence of the breach but nevertheless disputed its publicly-reported scope.

9. By December 21, 2020, however, Ledger could no longer cover up the data breach. On that day, the hacked customer list was posted publicly and became widely available. In a message posted on its website from its CEO, Ledger admitted to the scope of the attack, stating that the company "very deeply regret[s] this situation." Ledger's CEO further acknowledged that, as a result of the hack, "many [Ledger customers] have been targeted by e-mail and SMS phishing campaigns and that it's clearly a nuisance."

10. Ledger's and Shopify's misconduct has made targets of Ledger customers, with their identities known or available to every hacker in the world. Ledger's persistently deficient response compounded the harm. In failing to individually notify every affected customer or admit to the full scope of the breach, Ledger left customers unaware of the data breaches and concomitant hacking risks. The natural and foreseeable result was that many customers fell victim to hackers' phishing emails disguised as emails from Ledger.

11. Ledger customers would not have purchased Ledger wallets at all, or would not have paid as much as they did for Ledger wallets, had they known of Ledger's lax security practices and unwillingness to promptly and completely disclose data breaches.

12. Plaintiffs seek to redress Defendants' misconduct, occurring from April 1, 2020, to the present (the "Class Period"), under state common law and consumer-protection statutes on behalf of the Class and several Subclasses of Ledger customers affected by the data breach described herein.

II. PARTIES

Plaintiffs

13. Plaintiff John Chu is a resident of Georgia. He purchased and/or utilized devices and/or services from Ledger.

14. Plaintiff Edward Baton is a resident of Georgia. He purchased and/or utilized devices and/or services from Ledger.

Defendants

15. Defendant Ledger SAS is a French simplified joint-stock company headquartered in Paris, France.

16. Defendant Ledger Technologies Inc. is a wholly-owned subsidiary of Ledger SAS. It is incorporated in Delaware, registered to do business in California, and, at the time of the breach, was headquartered in San Francisco, California and has a substantial office at 121 2nd St #4, San Francisco, California 94105.

17. Defendant Shopify Inc. is a Canadian Corporation with offices at 151 O'Connor Street, Ground floor, Ottawa, Ontario, K2P 2L8.

18. Defendant Shopify (USA) Inc. is a Delaware corporation and registered to do business in California. Up until a week before it announced the data breach, its principal place of business was in San Francisco, California. It now lists Ottawa, Canada as its principal place of business. It is a wholly-owned subsidiary of Shopify Inc.

III. JURISDICTION AND VENUE

19. Jurisdiction of this Court is founded upon 28 U.S.C. § 1332(d) because the matter in controversy exceeds the value of $5,000,000, exclusive of interests and costs, there are more than 100 class members, and the matter is a class action in which any member of a class of plaintiffs is a citizen of a state different from any defendant.

20. This Court has personal jurisdiction over all parties.

21. Shopify (USA) Inc. is registered to do business in California, and for the vast-majority of the relevant time period, listed a California address as its principal place of business.

22. Similarly, Ledger Technologies is registered to do business in California has a substantial office at 121 2nd St #4, San Francisco, California 94105.

23. Ledger SAS dominates and controls Ledger Technologies' internal affairs and daily operations. Not only is Ledger Technologies a wholly-owned subsidiary of Ledger SAS, but there is substantial overlap among their executives. For example, the Chief Executive Officer ("CEO") of Ledger Technologies is Pascal Gauthier, who is also the Chairman and CEO of Ledger SAS. Ledger Technologies' secretary is listed as Antione Thibault, who is the general counsel of Ledger SAS.

Ledger Technologies' Chief Financial Officer ("CFO") is the CFO of Ledger SAS. Though Ledger SAS is not registered to do business in California, it boasts that it has employees in "Paris, Vierzon, and San Francisco" without differentiating between the two entities.

24. Shopify Inc. dominates and controls Shopify (USA) Inc.'s internal affairs and daily operations. Not only is Shopify (USA) a wholly-owned subsidiary of Shopify, but as in Ledger's case, there is a substantial overlap among its executives. Shopify (USA)'s CEO and CFO is Amy Shapero—the CFO of Shopify. The Secretary of Shopify (USA) is Shopify's Chief Legal Officer. In addition, Shopify's job listings notes that it will "hire you [ ] anywhere" as long as it has "an entity where you are." That is, Shopify does not differentiate between its entities for any job responsibilities and thus does substantial business through the American employees it hires through its subsidiary formerly located in California.

25. This Court also has personal jurisdiction over Shopify and Shopify (USA) because they solicit customers and transact business in California, including with Ledger and those who purchased products or services from Ledger.

26. This Court also has personal jurisdiction over Ledger and Ledger Technologies because they solicit customers, including Plaintiffs and Class members, in the United States and California. In fact, 33% of the compromised two hundred and seventy-three thousand accounts with address information belonged to Class members with U.S. addresses. This Court also has personal jurisdiction over Ledger and Ledger Technologies because Shopify (USA) acted as those entities' agent for the conduct giving rise to Plaintiffs' claims. With respect to the breached data of Ledger's customers, the responses to the breaches, and the conduct giving rise to Plaintiffs' causes of action, Ledger had the right to control the conduct of Shopify, which acted as Ledger's agent and was authorized to act on Ledger's behalf with respect to Ledger's customers.

IV. FACTUAL ALLEGATIONS

A. Bitcoin and Crypto-Assets

27. A crypto-asset is a digital asset designed to work as a medium of exchange or a store of value or both. Crypto-assets leverage a variety of cryptographic principles to secure transactions, control the creation of additional units, and verify the transfer of the underlying digital assets.

28. Bitcoin was the world's first decentralized crypto-asset. It is also the largest and most popular crypto-asset, with a market capitalization of approximately $1.08 billion. Bitcoin spawned a market of other crypto-assets that, together with Bitcoin, have a current market capitalization of approximately $1.94 trillion. (The term "bitcoin" can refer to both a computer protocol and a unit of exchange. Accepted practice is to use the term "Bitcoin" to label the protocol and software, and the term "bitcoin" to label the units of exchange.)

29. At its core, Bitcoin is a ledger of addresses and transfer amounts that tracks the ownership and transfer of every bitcoin in existence. This ledger is called the blockchain. The blockchain is completely public.

30. Blockchains act as the central technical commonality across most crypto-assets. While each blockchain may be subject to different technical rules and permissions based on the preferences of its creators, they are typically designed to achieve the similar goal of decentralization.

31. In April 2013, there were only seven crypto-assets listed on coinmarketcap.com, a popular website that tracks the crypto-asset markets. As of this filing, the site monitors more than 9,112 crypto-assets.

1. Transacting with Bitcoin and Blockchain Addresses

32. Because all blockchain addresses and transfers are public, the way to verify ownership of an address is through the use of public and private keys.

33. Each address has one public key and one private key associated with it. With the private key, one can control the address and can move bitcoin in or out of the account. The public key is more like a digital signature that is used to verify ownership and transfers of funds. The blockchain address, public key, and private key are often mathematically related to one another.

34. The private key is, however, the only mechanism that allows for the transfer of crypto-asset. With the private key—and nothing more—a person can implement an untraceable transfer of the crypto-asset from one digital address to another. Without the private key, the crypto-asset can never be transferred. In other words, anyone with the private key has total control over the funds. Thus, to safeguard crypto-assets, one must keep the private key private.

2. Security and Crypto-Assets

35. It is the cryptographic principals behind the use of public and private keys that give crypto-assets their name. Cryptography is at the heart of blockchain transactions, and security is one of the chief advantages and selling points of the technology.

36. Nonetheless, since the inception of crypto-assets, there have been high-profile hacks to steal them. One of the first large Bitcoin exchanges (handling over 70% of all Bitcoin transactions at the time) lost a staggering 850,000 bitcoins to theft, with a value exceeding $49 billion USD today.

37. It has been estimated that over $4 billion crypto-assets were lost to theft and related crimes in 2019.[1] That risk of theft continues today.

38. Because it is nearly impossible to guess a user's private key, hackers employ various methods to gain access to private keys. Once a hacker obtains the private key for an address, the hacker controls its funds. Unlike traditional accounts housed at banks, there are no approvals or fraud monitoring warnings for moving crypto-assets out of an account. Moreover, any transfer is effectively untraceable and irreversible, leaving the recipient immune from identification or claw-back.

39. Given this constant threat of theft, security over an individual's private keys is paramount.

B. Ledger and Hardware Wallets

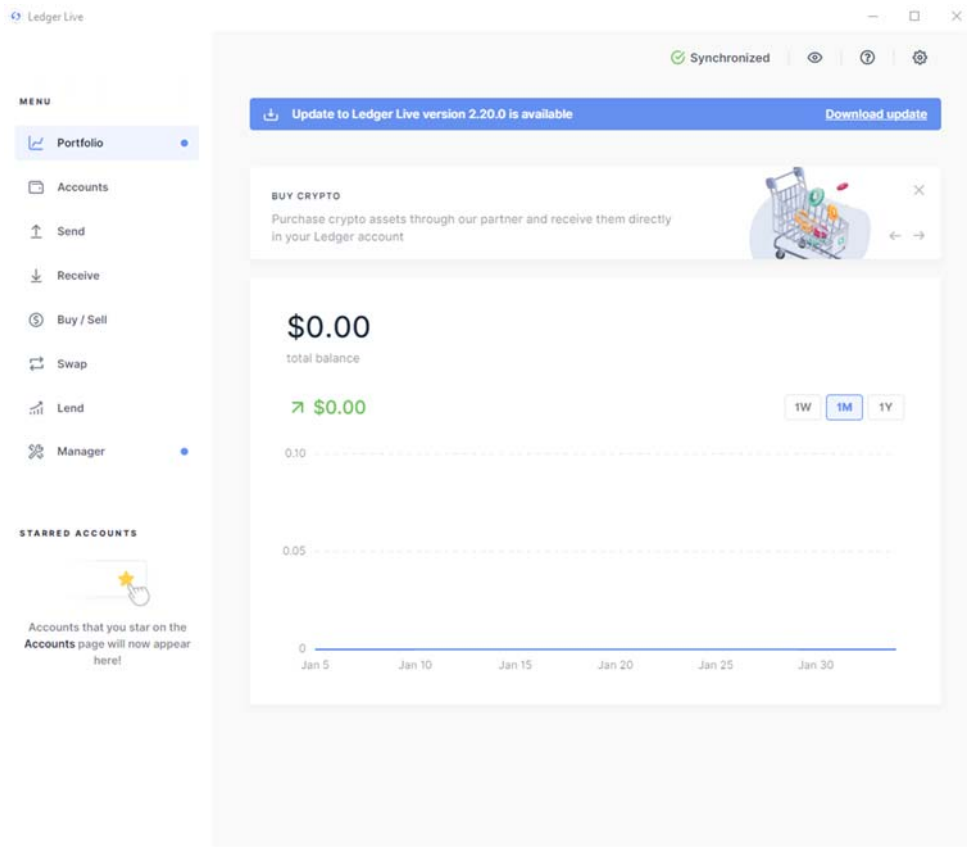
40. Ledger offers solutions to consumers to keep their crypto-assets safe. Ledger's main product offerings are "hardware wallets." These are physical consumer items that appear similar to a USB storage device. This is an example of a Ledger hardware wallet:

[1] Jeb Su, *Hackers Stole Over $4 Billion From Crypto Crimes In 2019 So Far, Up From $1.7 Billion In All Of 2018*, FORBES (Aug. 15, 2019, 01:49 PM EDT), https://www.forbes.com/sites/jeanbaptiste/2019/08/15/hackers-stole-over-4-billion-from-crypto-crimes-in-2019-so-far-up-from-1-7-billion-in-all-of-2018/?sh=42ef46855f58.

41. Despite being named a "wallet," such wallets do not "hold" cryptocurrency in the way a traditional wallet stores cash. Rather, consumers store their private keys on these physical devices, which are never connected to the internet (at least in the case of Ledger's products).

42. The wallet itself can be accessed only by entering a PIN. Simply misplacing the wallet thus poses no risk of theft. Ledger offers for sale two types of hardware wallets: the Ledger Nano S and the Ledger Nano X.

43. Ledger also produces "Ledger Live," a software product designed to interact with devices. This screenshot shows its core functionality, in that a user can use the software to buy, sell, send, and receive various crypto-assets:



44. Ledger has been highly successful selling these devices and services. Having raised $88 million in funding, it is one of the market leaders for crypto-asset security.

1. Hacking Hardware Wallets

45. Users of hardware wallets generally face discrete risks of theft by hacking because private keys exist only where the owners store them. If an owner stores the private keys only on a hardware wallet with no internet connectivity—and not on a personal computer—then traditional hacking cannot reveal those private keys. Instead, the main sources of risk are: (1) "phishing" attacks to trick a user into revealing the private PIN to their hardware wallet; or (2) physical intimidation that forces users into paying money or revealing that information to a hacker.

46. Phishing is the practice of purporting to be a legitimate institution and contacting targets with the goal of soliciting passwords, banking information, or other sensitive information. Common examples of this practice include mass spam emails sent to mimic the look and feel of a banking website. The email recipient receives the email, believes she needs to link to the account to update information, clicks a link in the email that goes to a sham website made to look like the real

bank website, and enters real login information into the sham website. The owners of the sham website then possess that victim's real banking login and password.

47. Internet users are becoming more and more savvy to phishing, however, requiring hackers to craft attacks that are increasingly realistic and personalized and less reliant on large-scale mass efforts.

48. Phishing attacks are also generally harder to accomplish against Ledger users, who are typically more skeptical and security conscious and, in turn, savvier to phishing practices. For example, Ledger users will commonly create special email addresses used just for interacting with accounts that manage their crypto assets. And Ledger users will often have a separate dedicated phone number to use for dual-factor authentication when interacting with their crypto assets.[2] These dedicated email addresses and phone numbers add another layer of protection to avoid phishing attacks. Users know that crypto-asset-related emails, texts, or calls to any "main" email address or phone number are illegitimate.

49. Similarly, using a separate phone number can protect users from other attacks, such as SIM swap attacks.[3] A SIM swap attack occurs when an attacker gains control of an individual's phone number by convincing the individual's mobile carrier to switch it to a new SIM card—one that the attacker possesses. Once attackers gain control of that phone number, they can then bypass dual-factor authentication requirements.

50. Plaintiffs—who have professional backgrounds, including in technology—were as savvy as anyone buying crypto assets and hardware wallets as far back as 2017. Accordingly, in addition to buying multiple Ledger products for storing their crypto assets, Plaintiffs took other precautions. Plaintiff Baton, for example, acquired a separate mobile phone and always interacted

[2] Dual authentication is a method in which a user is granted access to some system or device only after successfully presenting two or more pieces of evidence of rightful access, such as unique knowledge (*e.g.*, a password) or unique possession (*e.g.*, a key).

[3] SIM stands for "subscriber identification module," and a SIM card is a physical circuit that is used to securely store the unique identifier of any user on a cellular network.

with crypto assets using a virtual private network to encrypt communications and shield his IP address.

51. As to physical intimidation, even the savviest internet user cannot insulate himself from such threats. A hacker can contact an owner of crypto-assets and threaten the owner with physical violence unless an effective ransom is paid (usually in the form of an untraceable transfer of crypto-assets transfer to the hacker). These threats are rare. Without knowing an owner's home address, physical location, or even phone number, a hacker would have difficulty making a credible threat prompting payment from the victim. And hackers cannot identify viable targets by simply looking up publicly listed names, phone numbers, and addresses. Crypto-assets have not yet been widely adopted; therefore, attackers have no way of knowing whether would-be targets own crypto-assets or hardware wallets. In addition, for owners of crypto-assets, there is no analog for the physical bank ATM—where would-be attackers could potentially wait, identify victims with funds, and intimidate those victims.

52. For these reasons, the single greatest point of vulnerability for owners of Ledger wallets is public disclosure of the information that a particular person owns the wallet. If hackers know the names and/or email addresses of people who own Ledger wallets, then hackers can target those people with sophisticated phishing schemes and tailored threats.

53. Accordingly, by operating in the crypto-asset security space, Ledger places itself between user's funds and would-be hackers. The anonymity of its customer list is a key and obvious element of the security that Ledger offers. By analogy, a manufacturer of state-of-the-art lock safes would not publish its customer list, which is valuable to would-be thieves seeking to identify targets possessing high-value items. Similarly, public disclosure of Ledger's customers puts those individuals in the crosshairs of the very hackers the company seeks to impede.

2. Ledger Advertises State-of-the-Art Security for Crypto-Assets

54. Ledger's consistent message to consumers is that Ledger wallets offer the best possible protection for crypto-assets. Their tagline embodies this value proposition: "If you don't want to get hacked, get a Ledger wallet." Ledger represented to consumers, prior to the data breach at issue, the following:

> Critical digital assets are the new oil and securing them is the most important challenge for the coming years.
>
> That's where we come in. We are Ledger.
>
> We are a unique digital security ecosystem that provides protection and is *built on verifiable trust across our people, hardware and software.* And in today's world, we know that trust deserves proof. This is why we provide transparency into how our technology works.
>
> *We relentlessly stress-test our own technology solutions*. Our Ledger Donjon team is made up of world-class experts with extensive backgrounds in the security and smartcard industries. *They continuously look for vulnerabilities on Ledger products as well as our providers' products in an effort to analyze and improve the security. We know security means never standing still.*

(emphasis added).

55. Ledger further and publicly asserted, prior to the data breach at issue:

- "At Ledger we are developing hardware wallet technology that provides the highest level of security for crypto assets;"
- "Ledger hardware wallet, combined with the Ledger Live application, is the best solution to secure and control your crypto assets;"
- "Ledger hardware wallets are designed with the highest security standard to keep your crypto secure at all time;"
- "Ledger enables resilience through verifiable trust. Knowing trust is the greatest way to make our world truly move forward and progress."

56. Ledger also republished, prior to the data breach at issue, acknowledgments from reputable third-party commentators:

- "French Crypto Wallet Ledger Is Solving Bitcoin's Biggest Flaw" (as featured in Forbes);
- "Ledger makes sure private keys never become accessible to thieves, online or anywhere else" (as featured in Bloomberg);
- "Ledger removes the risk of being hacked" (as featured on CNBC).

57. Through those statements, Ledger conveyed to consumers that Ledger wallets, coupled with Ledger's services, provide the highest standard of security for owners of crypto-assets. Ledger further conveyed that it was tirelessly assessing its wallets and supporting services for

vulnerabilities, while adapting to protect against those threats. By buying a Ledger wallet, consumers purportedly were buying into a comprehensive security support system that maximized protections against threats to crypto-assets.

58. Making the forgoing, unequivocal representations, Ledger sold Class members the Ledger Nano X wallet for $119 and the Ledger Nano S wallet for $59. Class members would not have purchased these products at all, or would have paid significantly less for them, had they known of Ledger's lax security practices and unwillingness to promptly and completely disclose data breaches.

3. Ledger Uses Shopify as an E-commerce Vendor

59. Ledger sells its Nano products through a number of distributors, including retailers like Amazon and Walmart. It also sells directly to consumers through https://shop.ledger.com/ (the "Shopping Website").

60. Shopify powers Ledger's Shopping Website. Shopify is an e-commerce giant. Over one million businesses use its platform, and over $61 billion of sales occurred on its platform through these businesses in 2019. It is the largest publicly-traded company in Canada.

61. Shopify's success is based on providing services to allow companies to easily operate online stores. Shopify provides e-commerce solutions for businesses to allow them to easily create digital storefronts. For example, Shopify allows you to create a well-designed web layout, provides a payment provider to accept credit card payments, and makes various profit and inventory applications available. These solutions are essentially a software product that companies subscribe to in order to host digital stores.

62. When users purchase directly from Ledger on its Shopping Website, they must provide certain personal information before placing an order, such as their physical address, phone number, and email address. Because Ledger uses Shopify's services, Shopify acts as an intermediary between Ledger and purchasers of Ledger's products. Therefore, Shopify also has access to the personal information that purchasers provide.

63. Shopify's terms of service obligate it to "take all reasonable steps" to protect the disclosure of confidential information, including "names, addresses and other information regarding customers and prospective customers."

C. The Ledger Data Breach

64. In mid-2020, between April and June, certain Shopify employees took advantage of Shopify's access to the personal information of Ledger's customers and acquired and exported Ledger's customer transactional records (the "Data Breach"). The Shopify employees also obtained data relating to other merchants.

65. On September 22, 2020, Shopify announced that: (1) "two rogue members of our support team were engaged in a scheme to obtain customer transactional records of certain merchants;" (2) the "incident involv[ed] the data of less than 200 merchants;" and (3) "Our teams have been in close communication with affected merchants to help them navigate this issue and address any of their concerns." This announcement made it clear that Shopify was aware of the data breach before the day of the announcement and even had time to "conduct an investigation" and notify affected merchants. On information and belief, Shopify knew of the data breach more than one week before.

66. On information and belief, those rogue employees were located in America, as immediately after noting that the employees' access was terminated, Shopify's statement highlighted its compliance with *American* (rather than Canadian) legal authorities in stating that it was "currently working with the FBI and other international agencies." To the extent these employees were American, they were most probably employed by its California office.

67. The Data Breach in fact involved the data of approximately 272,000 people,[4] approximately a third of whom live in the United States.[5] Hackers copied information such as names,

[4] *E-commerce and Marketing data breach – FAQ*, LEDGER, https://support.ledger.com/hc/en-us/articles/360015559320-E-commerce-and-Marketing-data-breach-FAQ (last visited Apr. 5, 2021).

[5] Larry Cermak, *A detailed look at the Ledger data leak and other recent incidents*, THE BLOCK (Dec. 21, 2020, 9:49 AM EST), https://www.theblockcrypto.com/genesis/88706/a-detailed-look-at-the-ledger-data-leak-and-other-recent-incidents.

order details, email addresses, physical addresses, and phone numbers.[6] And for many more users, hackers obtained the email address users used when buying their Ledger.[7]

68. By the time it publicly announced the breach, Shopify notified every affected merchant that rogue employees had stolen their data, but neither Shopify nor Ledger warned the hundreds of thousands of vulnerable Ledger customers harmed by the Data Breach. Instead, as the timeline below explains, Ledger attempted to cover up and downplay the scale of the Data Breach.

1. April – June 2020: Ledger Initially Denies the Data Breach

69. In May 2020, public rumors arose concerning the Data Breach. The rumors were that Ledger's consumer information from Shopify had been hacked.[8]

70. This publicly-stated concern was an opportunity for Ledger to get ahead of the problem. Ledger should have, at a minimum: (1) disclosed the breach; (2) notified all impacted and potentially impacted users; (3) offered services to help impacted users transition to new accounts; (4) monitored for suspicious transactions; (5) hired third-party auditors to conduct security testing; (6) trained employees to identify and contain similar breaches; and (7) trained and educated their users about the threats they faced.

71. Instead, Ledger's immediate reaction was to deny that there was a breach impacting Ledger's customers. Ledger stated that "**Rumors pretend** our Shopify database has been hacked through a Shopify exploit. Our e-commerce team is currently checking these allegations by analyzing the so-called hacked [database], and so far **it doesn't match** our real [database]. We

---

[6] *Id.*

[7] *Id.*

[8] Jamie Redman, *Hacker Attempts to Sell Data Allegedly Tied to Ledger, Trezor, Bnktothefuture Customers*, BITCOIN (May 24, 2020), https://news.bitcoin.com/hacker-attempts-to-sell-data-allegedly-tied-to-ledger-trezor-bnktothefuture-customers/.

@UnderTheBreach, TWITTER (May 24, 2020, 03:39 AM) https://twitter.com/underthebreach/status/1264460979322138628?ref_src=twsrc%5Etfw%7Ctwcamp%5Etweetembed%7Ctwterm%5E1264460979322138628%7Ctwgr%5E%7Ctwcon%5Es1_&ref_url=https%3A%2F%2Fnews.bitcoin.com%2Fhacker-attempts-to-sell-data-allegedly-tied-to-ledger-trezor-bnktothefuture-customers%2F.

continue investigations and are taking the matter seriously."[9] During this time, the risks and damages to Ledger's customers were only increasing; a prompt and proper response from Ledger, including full disclosure to all customers, would have mitigated those risks and damages.

2. July 2020: Ledger Admits the Data Breach Occurred, but Downplays Its Scale

72. On July 29, 2020, Ledger made partial admissions that exacerbated, rather than mitigated, the harm caused by the Data Breach.

73. After researchers informed Ledger of a potential data breach on its website, Ledger announced that its marketing and e-commerce database had been exposed in June 2020:

> **What happened**
> On the 14th of July 2020, a researcher participating in our bounty program made us aware of a potential data breach on the Ledger website. We immediately fixed this breach after receiving the researcher's report and underwent an internal investigation. A week after patching the breach, we discovered it had been further exploited on the 25th of June 2020, by an unauthorized third party who accessed our e-commerce and marketing database – used to send order confirmations and promotional emails – consisting mostly of email addresses, but with a subset including also contact and order details such as first and last name, postal address, email address and phone number. **Your payment information and crypto funds are safe.**
>
> To be as transparent as possible, we want to explain what happened. An unauthorized third party had access to a portion of our e-commerce and marketing database through an API Key. The API key has been deactivated and is no longer accessible.
>
> **What personal information was involved?**
> Contact and order details were involved. This is mostly the email address of our customers, approximately 1M addresses. Further to investigating the situation we have also been able to establish that, for a subset of 9500 customers were also exposed, such as first and last name, postal address, phone number or ordered products. Due to the scope of this breach and our commitment to our customers, we have decided to inform all of our customers about this situation.
>
> Those 9500 customers whose detailed personal information are exposed will receive a dedicated email today to share more details.
>
> **Regarding your ecommerce data, no payment information, no credentials (passwords), were concerned by this data breach. It solely affected our customers' contact details**.

[9] @Ledger, TWITTER (May 24, 2020 06:39 AM), https://twitter.com/Ledger/status/1264506360735174657.

> **This data breach has no link and no impact whatsoever with our hardware wallets nor Ledger Live security and your crypto assets, which are safe and have never been in peril. You are the only one in control and able to access this information**.

(emphasis in original).

74. Ledger's disclosure and responsive measures were flawed and misleading.

75. *First*, as Ledger admitted, it failed to immediately warn its customers and instead waited on the results of its "internal investigation with third party experts before warning [its] community."[10] This delay in issuing even a warning was reckless, or at least negligent.

76. *Second*, Ledger did not disclose that this breach had anything to do with the Shopify breaches, which involved insiders stealing information for personal profit. Ledger never even mentioned Shopify. This incomplete disclosure was reckless, or at least negligent.

77. *Third*, Ledger was not clear as to the status and dissemination of the stolen data. Ledger explained that "[w]e are actively monitoring for evidence of the database being sold on the internet, and have found none thus far." Ledger also explained that they "immediately fixed this breach" and were undertaking an "internal investigation," choosing to eschew third party auditors. Ledger also took pains to repeatedly reiterate to consumers that the breach had "no impact whatsoever with our hardware wallets nor Ledger Live security and your crypto assets." In other words, Ledger's message was that, after an exhaustive internal investigation, they had identified a limited hack and had rectified the situation. This patently inaccurate disclosure was reckless, or at least negligent.

78. *Fourth*, Ledger sent follow-up notifications only to the 9,500 customers whom they determined had additional personal information exposed. In doing so, Ledger failed to notify its one million other customers whose email information had been exposed. This patently incomplete follow-up was reckless, or at least negligent.

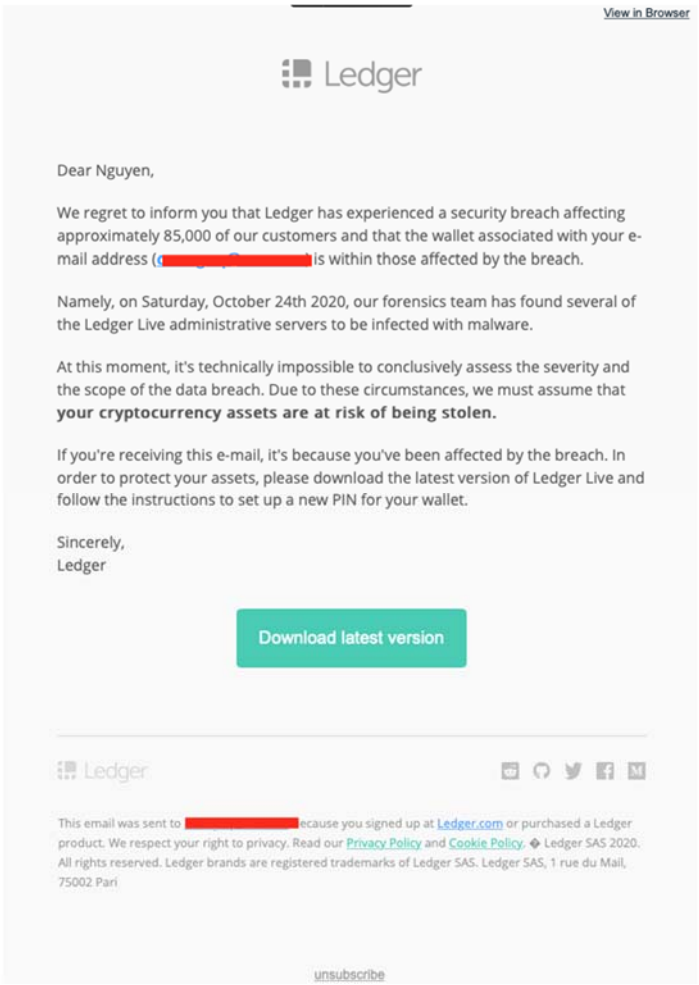
---

[10] *Addressing the July 2020 e-commerce and marketing data breach — A Message From Ledger's Leadership*, LEDGER (July 29, 2020), https://www.ledger.com/addressing-the-july-2020-e-commerce-and-marketing-data-breach.

3. August – December 2020: Hacking Attacks Increase on Ledger Users

79. By the fall of 2020, Ledger and Shopify were still failing to respond appropriately to the severe threats that customers faced or to the damages they had incurred. Ledger still had not disclosed that its customers had any connection to the Shopify breaches. It had not contacted every customer whose email address had been exposed to hackers. It had not provided sufficient disclosures or resources to assist customers in protecting against rising phishing schemes. Meanwhile, several media reports signaled that Ledger's customers were under attack as a result of the Data Breach.

80. In October 2020, for example, a Ledger user reported a phishing attempt by hackers posing as Ledger Support team members and asking Ledger customers to download fake versions of the Ledger Live software. The fake email looked very convincing:



View in Browser

Ledger

Dear Nguyen,

We regret to inform you that Ledger has experienced a security breach affecting approximately 85,000 of our customers and that the wallet associated with your e-mail address ([redacted] is within those affected by the breach.

Namely, on Saturday, October 24th 2020, our forensics team has found several of the Ledger Live administrative servers to be infected with malware.

At this moment, it's technically impossible to conclusively assess the severity and the scope of the data breach. Due to these circumstances, we must assume that **your cryptocurrency assets are at risk of being stolen.**

If you're receiving this e-mail, it's because you've been affected by the breach. In order to protect your assets, please download the latest version of Ledger Live and follow the instructions to set up a new PIN for your wallet.

Sincerely,
Ledger

Download latest version

Ledger

This email was sent to [redacted] because you signed up at Ledger.com or purchased a Ledger product. We respect your right to privacy. Read our Privacy Policy and Cookie Policy. ◆ Ledger SAS 2020. All rights reserved. Ledger brands are registered trademarks of Ledger SAS. Ledger SAS, 1 rue du Mail, 75002 Pari

unsubscribe

81. Other Ledger users responded to the report by confirming that they had received and been tricked by the fake email. One user reported: "Wow this looked really legit, so much so I used Contact Us form to ask Ledger if it was real. I am normally pretty good at sniffing things like this out – this was by far the most convincing attempt I have ever seen."[11]

82. The hackers behind this fake email were of course armed with Ledger's customer lists and email addresses and, therefore, knew they were targeting Ledger owners. Accordingly, the hackers invested the time and resources to create such a convincing—and, unfortunately, successful—fake. Worse yet, because of Ledger's false and misleading statements and omissions regarding the Data Breach, Ledger's customers did not know that their email had been compromised. Ledger thus deprived them of the opportunity to increase their wariness and/or take other precautions to avoid such hacking.

83. The phishing attempts were not limited to emails. Ledger users began to report the receipt of SMS/text phishing messages, again claiming to be from Ledger, such as the below:

[11] Benjamin Powers, *'Convincing' Phishing Attack Targets Ledger Hardware Wallet Users*, COINDESK (Oct. 27, 2020, 04:13 PM EDT, updated Nov. 2, 2020, 02:56 PM EST), https://www.coindesk.com/phishing-attack-ledger-cryptocurrency-wallet.

84. Other hackers used a different phishing attempt, attempting to pose not as Ledger, but as other entities such as the Stellar Development Foundation ("Stellar"), an entity affiliated with the creator of the Stellar Lumen token purchased by Plaintiff Baton. Under this scheme, hackers sent an extremely sophisticated email posing as Stellar and soliciting users such as Baton to "stake" Stellar Lumen tokens—a well-known form of deposit that pays interest.

85. These emails and websites were effective in part because they looked like Stellar's actual website, using real assets, articles, features, and other content from Stellar's email and website. In order to stake Lumens, a user would have to transfer the Lumens to a staking address. But the staking "address" provided to deposit the funds was not actually associated with Stellar, and once the funds were transferred, the hackers absconded with it. Critically, this phishing strategy did not require the disclosure of any private keys and increased a victim's trust in the malicious site.

86. Creating such convincing versions of Stellar's website and emails required a significant amount of effort, which paid off because the hackers knew they could target the emails of likely cryptocurrency holders such as Plaintiff Baton.

87. In response to these reports, Ledger should have devoted substantial resources and taken responsibility for being the source of the leak that allowed this precision targeting from hackers. Instead, Ledger continued to tout its security credentials and prevaricated about whether the increased phishing and hacking attempts arose from a data breach.

88. On November 2, 2020, Ledger refused to acknowledge the Data Breach was the source of the rising attacks on its customers:

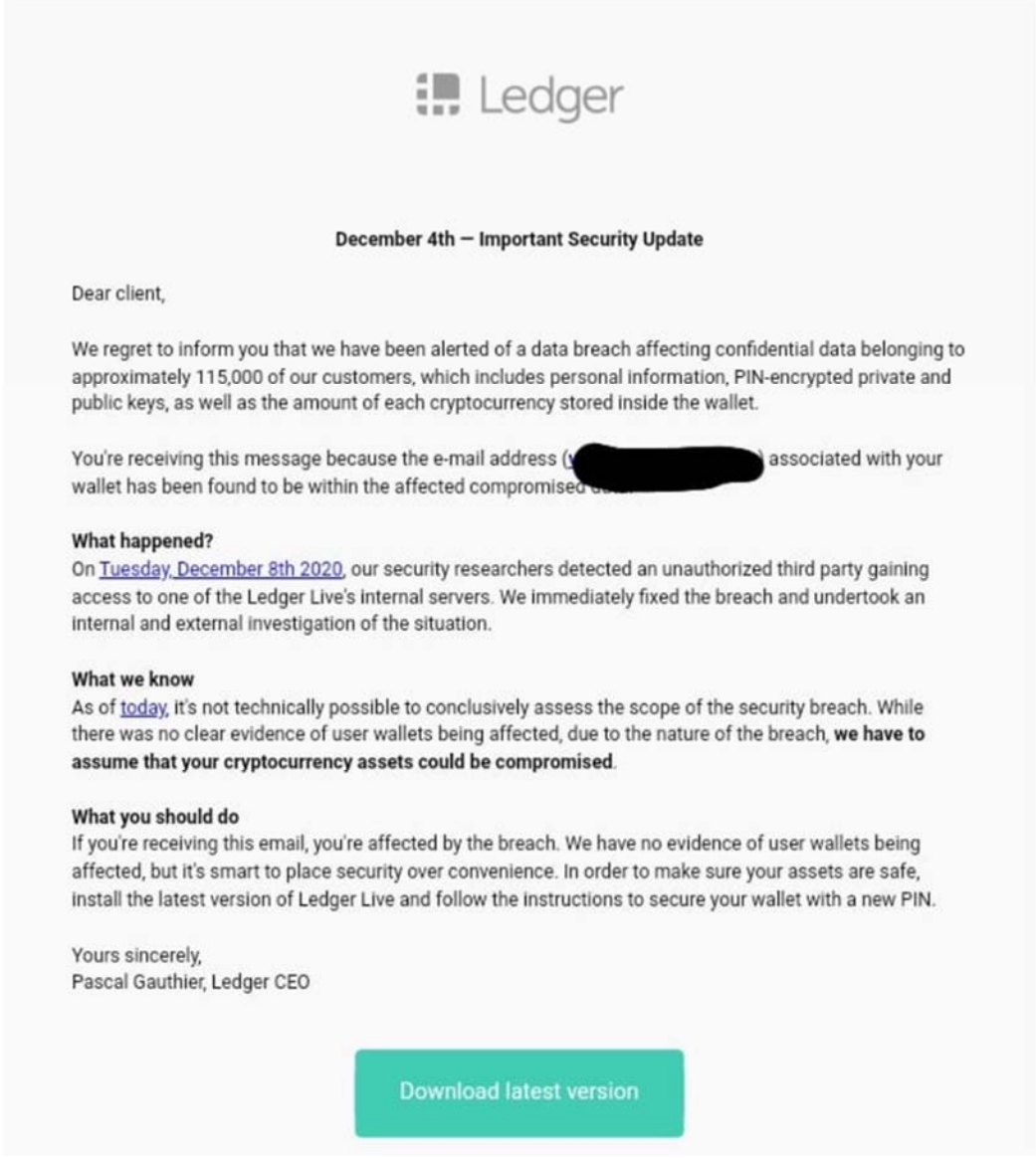
> As soon as we discovered the data breach on Ledger's website in July 2020, we immediately patched it. Since then, we led two penetration tests with a third-party consultancy to verify and improve the security of our clients' data. For two weeks, some of Ledger's customers have been experiencing continuous phishing scams through various channels, including email and SMS. We've issued several scam alerts through our Twitter, email, and other channels to notify our users during the past two weeks.
>
> The internal task force is investigating these attacks, and as of now, **we can't state that scammers are using Ledger's marketing database**, and therefore, these attacks resulted from July's data breach.[12]

89. Ledger's efforts to cover up and downplay the actual and potential scale of the Data Breach in the months leading up to its widespread public disclosure caused disastrous harm to its customers. During that time, many crypto-asset investors lost massive sums of money. Had Ledger acted responsibly during this period, much of that loss could have been avoided.

4. December 2020: In the Face of Widespread Public Disclosure, Ledger Admits to the Scale of the Data Breach

90. By early December 2020, reports continued to escalate about phishing attempts on Ledger's users. By that time, Ledger's inaction had provided an opportunity for the hackers to increase the sophistication and effectiveness of phishing attempts. For example, some of the phishing attempts referenced breaches and then instructed users, as a security measure, to install fake versions of Ledger Live that asked for their private key information:

[12] Benjamin Powers, *'Convincing' Phishing Attack Targets Ledger Hardware Wallet Users*, COINDESK (Oct. 27, 2020, 04:13 PM EDT, updated Nov. 2, 2020, 02:56 PM EST), https://www.coindesk.com/phishing-attack-ledger-cryptocurrency-wallet.



Ledger

December 4th — Important Security Update

Dear client,

We regret to inform you that we have been alerted of a data breach affecting confidential data belonging to approximately 115,000 of our customers, which includes personal information, PIN-encrypted private and public keys, as well as the amount of each cryptocurrency stored inside the wallet.

You're receiving this message because the e-mail address ([redacted]) associated with your wallet has been found to be within the affected compromised [redacted].

What happened?
On Tuesday, December 8th 2020, our security researchers detected an unauthorized third party gaining access to one of the Ledger Live's internal servers. We immediately fixed the breach and undertook an internal and external investigation of the situation.

What we know
As of today, it's not technically possible to conclusively assess the scope of the security breach. While there was no clear evidence of user wallets being affected, due to the nature of the breach, **we have to assume that your cryptocurrency assets could be compromised**.

What you should do
If you're receiving this email, you're affected by the breach. We have no evidence of user wallets being affected, but it's smart to place security over convenience. In order to make sure your assets are safe, install the latest version of Ledger Live and follow the instructions to secure your wallet with a new PIN.

Yours sincerely,
Pascal Gauthier, Ledger CEO

Download latest version

91. Users reported losing significant sums of crypto-assets as a result of such phishing. Plaintiff Chu lost about 4.2 bitcoin and 11 ether, collectively worth approximately $267,000 at today's market prices. Plaintiff Baton lost about 150,000 Stellar Lumens, worth approximately $72,000 at today's market prices.

92. The phishing attempts were sufficiently successful—and notorious—so that, through December 20, 2020, the going rate among hackers for the compromised list of Ledger customer data was approximately $100,000.[13]

[13] @UnderTheBreach, TWITTER (Dec. 20, 2020, 01:38 PM),

93. On December 20, 2020, a hacker published the Ledger customer data online. This publication included the personal information of more than 270,000 Ledger customers.

94. Consumers and reporters were quick to criticize Ledger, stating that the company had "vastly underestimated" the Data Breach in its prior statements.[14]

95. With the data made publicly available for free, many Ledger customers started receiving frightening threats. Ledger customers immediately started receiving spam phone calls, emails, and even death threats. Many of these customers shared their experiences online:

96. Plaintiffs Chu, Baton, and Shillito, like many members of the Class, also received spam emails, phone calls, and texts which, *inter alia,* attempted to phish for additional personal information and sell prurient content.

97. Ledger knew of and advertised the importance of protecting its customers' personal information, but before and after the Data Breach, it failed to take reasonable steps to protect its

---

https://twitter.com/UnderTheBreach/status/1340735356375851009.

[14] Vishal Chawla, Liam Kelly, *Ledger Breach Vastly Underestimated, 270,000 Clients Data Leaked*, CRYPTO BRIEFING (Dec. 21, 2020), https://cryptobriefing.com/ledger-breach-clients-data-leaked/.

customers. Before the breach, Ledger should have regularly deleted or archived customer data or should have otherwise protected that information from online accessibility. After the breach, Ledger repeatedly failed to provide critical information to its customers, compounding the harm to Plaintiffs and the Class.

98. Shopify similarly failed to protect Ledger's customer data. Shopify employees, rogue or not, had no need for direct access to Ledger customer data. Shopify should have: (1) limited employee access to customers' data in a way that prevented the rogue employees' access; (2) monitored employees' suspicious copying of customer data; (3) assisted Ledger with its investigation to determine the scope of the Data Breach; and (4) notified Ledgers' users of the Data Breach.

D. Plaintiffs Suffered Damages

99. Plaintiffs Chu and Baton have suffered damages from the Data Breach.

100. As to direct monetary losses, Plaintiff Chu lost about 4.2 bitcoin and 11 ether, collectively worth approximately $267,000 at today's market prices. Plaintiff Baton lost about 150,000 Stellar Lumens, worth approximately $72,000 at today's market prices.

101. If Ledger had timely disclosed the extent of the Data Breach, Plaintiffs—sophisticated users with technology backgrounds and wary of scams—would have been on heightened alert and not fallen prey to these scams.

102. As to other forms of damages, Plaintiff Chu had his email compromised and has received several spam messages since his email was leaked. Plaintiff Baton had his email, physical address, and phone number compromised. He received regular spam calls, still receives spam emails and had to change his phone number and where he receives packages as a result of this breach. He also remains fearful of intruders due to his physical address being publicly leaked.

103. These leaks of personal information, in conjunction with the information that they were Ledger customers, have exposed Plaintiffs to additional risks of theft and threat.

104. In addition, Plaintiffs would not have purchased Ledger's products at all, or would have paid significantly less for them, had they known of Ledger's lax security practices and unwillingness to promptly and completely disclose data breaches.

V. CLASS ALLEGATIONS

105. Plaintiffs bring this Action as a class action pursuant to Fed. R. Civ. P. 23 and seek certification of the following Class and Subclasses:

> Nationwide Class: All persons residing in the United States who provided Ledger or Shopify with personal information that was accessed, compromised, stolen, or exposed in a data breach between April 1, 2020, and the present.
>
> Nationwide Phishing Subclass: All persons in the Class who suffered monetary damages in connection with a phishing or threatening communication by a third-party possessing those persons' personal information disclosed as a result of a data breach between April 1, 2020, and the present.
>
> Nationwide Consumer Class: All persons residing in the United States who purchased a Ledger Nano X wallet or a Ledger Nano S wallet from Ledger or an authorized reseller within the limitations period, as may be extended or tolled by any applicable rule of law or equitable doctrine.
>
> California Subclass: All persons residing in California who provided Ledger or Shopify with personal information that was accessed, compromised, stolen, or exposed in a data breach between April 1, 2020, and the present.
>
> California Phishing Subclass: All persons in the California Subclass who suffered monetary damages in connection with a phishing or threatening communication by a third-party possessing those persons' personal information disclosed as a result of a data breach between April 1, 2020, and the present.
>
> California Consumer Subclass: All persons residing in California who purchased a Ledger Nano X wallet or a Ledger Nano S wallet from Ledger or an authorized reseller within the limitations period, as may be extended or tolled by any applicable rule of law or equitable doctrine.
>
> Georgia Subclass: All persons residing in Georgia who provided Ledger or Shopify with personal information that was accessed, compromised, stolen, or exposed in a data breach between April 1, 2020, and the present.
>
> Georgia Phishing Subclass: All persons in the Georgia Subclass who suffered monetary damages in connection with a phishing or threatening communication by a third-party possessing those persons' personal information disclosed as a result of a data breach between April 1, 2020, and the present.
>
> Georgia Consumer Subclass: All persons residing in Georgia who purchased a Ledger Nano X wallet or a Ledger Nano S wallet from Ledger or an authorized reseller within the limitations period, as may be extended or tolled by any applicable rule of law or equitable doctrine.

Accordingly, the Class Period is April 1, 2020, through the present except as to the Consumer

Subclasses.

106. Excluded from the Class and Subclasses are Defendants, their officers and directors, and members of their immediate families or their legal representatives, heirs, successors or assigns and any entity in which Defendants have or had a controlling interest.

107. Plaintiffs reserve the right to amend the Class definition if investigation or discovery indicate that the definition should be narrowed, expanded, or otherwise modified.

108. The Class members are so numerous that joinder of all members is impracticable. The precise number of Class members is unknown to Plaintiffs at this time, but it is believed to be in the tens of thousands.

109. The Class members are readily ascertainable and identifiable. They may be identified through contact information that was breached. They may be notified of the pendency of this Action by electronic mail using a form of notice customarily used in class actions.

110. Plaintiffs' claims are typical of the claims of the Class members, who are similarly affected by Defendants' respective wrongful conduct in violation of the laws complained of herein. Plaintiffs do not have any interest that is in conflict with the interests of the Class members.

111. Plaintiffs and the Class members sustained damages and/or are entitled to restitution from data exposure caused by Defendants' unlawful conduct and/or for the diminution in value of the products they purchased revealed by Defendants' unlawful conduct.

112. Plaintiffs have fairly and adequately protected, and will continue to fairly and adequately protect, the interests of the Class members and have retained counsel competent and experienced in class actions and data privacy litigation. Plaintiffs have no interests antagonistic to or in conflict with those of the Class.

113. Common questions and answers of law and fact exist as to all Class members and predominate over any questions solely affecting individual Class members, including but not limited to the following:

- The precautions that Defendants took and failed to take with respect to the protection of the Class members' data;
- The steps Defendants took and failed to take after learning of the Data Breach and the reasonableness of those steps;

- The duties Defendants owed to the Class members, and the manner in which they breached those duties;
- The economic value of Ledger's wallets and services as advertised;
- The actual economic value of Ledger's wallets and services where, contrary to its advertising, Ledger failed to protect customers' personal information from nefarious actors;
- The quantification of the harm to Class members resulting from the exposure of their data to prospective hacking; and
- The restitution and/or damages to which Class members are entitled as result of the fact that the actual value of the Ledger wallets was far less than the value of the wallets as advertised.

114. A class action is superior to all other available methods for the fair and efficient adjudication of this controversy since joinder of all members is impracticable. Furthermore, as the damages suffered by some of the individual Class members may be relatively small, the expense and burden of individual litigation makes it impossible for Class members to individually redress the wrongs done to them.

115. There will be no difficulty in the management of this Action as a class action.

VI. CLAIMS FOR RELIEF

FIRST CAUSE OF ACTION

NEGLIGENCE

(On Behalf of Plaintiffs, the Nationwide Class, and the Nationwide Phishing Subclass and, Alternatively, on Behalf of the Remaining Non-Consumer Subclasses)

116. Plaintiffs incorporate the preceding paragraphs.

117. Ledger and Shopify owed a duty to the Class members, including Plaintiffs, to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting their personal information in their possession from being compromised, lost, or stolen, and from being accessed, and misused by unauthorized persons.

118. This duty included: (a) designing, maintaining, and testing Ledger's and Shopify's security systems to ensure that the Class members' personal information was adequately secured

and protected; (b) implementing processes that would timely detect a breach of their security systems; (c) timely acting upon warnings and alerts, including those generated by their own security systems, regarding intrusions to their networks; (d) maintaining data-security measures consistent with industry standards; and (e) timely and comprehensively notifying Class members of any potential or actual unauthorized access of their personal information.

119. Ledger's and Shopify's duties to use reasonable care arose from several sources, including those described below. Ledger and Shopify had a common law duty to prevent foreseeable harm to others, including Class members, who were the foreseeable and probable victims of any inadequate security practices. Ledger and Shopify in fact knew that their failure to protect Class members' personal information would likely harm Class members, because they knew that hackers routinely attempt to steal such information and use it for nefarious purposes.

120. Ledger's and Shopify's duties also arose under Section 5 of the Federal Trade Commission ("FTC") Act, 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, failing to use reasonable measures to protect personal information by companies such as Ledger. Various FTC publications and data security breach orders further form the basis of Ledger's and Shopify's duties. In addition, individual states have enacted statutes based upon the FTC Act that also created a duty.

121. Ledger's and Shopify's duties also arose from Ledger's unique position in the burgeoning crypto-asset market. Ledger strove to create "the highest level of security for crypto assets," and Ledger was in a unique and superior position to protect against the harm to the Class members as a result of data breaches. As Ledger's e-commerce vendor entrusted with Ledger's data, Shopify was in the same unique and superior position to protect against this harm.

122. Ledger and Shopify also had duties to safeguard the personal information of the Class members and to promptly notify them of a breach because of state laws and statutes that require Ledger to reasonably safeguard sensitive personal information. Timely notification was necessary to permit Class members to take appropriate measures to protect their identities as owners of crypto-assets, safeguard against threats to those crypto-assets, safeguard against personal threats, and take other steps to mitigate or ameliorate the damages caused by Ledger's and Shopify's misconduct.

123. Ledger and Shopify breached their duties to the Class members and thus were negligent. Ledger and Shopify breached these duties by, among other things, failing to: (a) exercise reasonable care and implement adequate security systems, protocols, and practices sufficient to protect the personal information of the Class members; (b) detect the breaches while they were ongoing; (c) maintain security systems consistent with industry standards; and (d) disclose that the Class members' personal information in Ledger's and/or Shopify's possession had been or was reasonably believed to have been stolen or compromised.

124. Ledger's and Shopify's negligence was, at least, a substantial factor in causing the Class members' personal information to be improperly accessed, disclosed, and otherwise compromised, and in causing the Class members' other injuries as a result of the data breaches.

125. As a direct and proximate result of Ledger's and Shopify's negligence, the Class members are entitled to damages, including compensatory, punitive, and nominal damages, in an amount to be proven at trial, for injuries that include at least the following:

a. the theft of their personal information;

b. the diminished value and loss of the benefits of purchased Ledger devices, which now pose a security risk to the Class members;

c. the costs associated with the detection and prevention of phishing scams aimed at depriving the Class members of assets and funds;

d. the costs associated with purchasing new hardware and software to protect crypto assets and/or other assets and/or funds;

e. the costs associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate, mitigate, and deal with the actual and future consequences of the data breaches;

f. the imminent and impending injury flowing from potential fraud and theft posed by their personal information being placed in the hands of criminals;

g. the mental anguish from the stress and fear of receiving threats and other messages from internet users who have physical address information;

h. the damages to and diminution in value of their personal information entrusted,

directly or indirectly, to Ledger with the mutual understanding that Ledger would safeguard the Class members' data against theft and not allow access and misuse of their data by others; and

i. the continued risk of exposure to hackers and thieves of their personal information, which remains in Ledger's possession and is subject to further breaches so long as Ledger fails to undertake appropriate and adequate measures to protect the Class members.

SECOND CAUSE OF ACTION

NEGLIGENCE PER SE
(On Behalf of Plaintiffs, the Nationwide Class, and the Nationwide Phishing Subclass and, Alternatively, on Behalf of the Remaining Non-Consumer Subclasses)

126. Plaintiffs incorporate the preceding paragraphs.

127. Section 5 of the FTC Act, 15 U.S.C. § 45, prohibits "unfair . . . practices in or affecting commerce" including, as interpreted and enforced by the FTC, the unfair act or practice by companies such as Ledger of failing to use reasonable measures to protect personal information. Various FTC publications and orders also form the basis of Ledger's and Shopify's duties.

128. Ledger and Shopify violated Section 5 of the FTC Act (and similar state statutes) by failing to use reasonable measures to protect personal information and not complying with industry standards. Ledger's and Shopify's conduct was particularly unreasonable given the nature and amount of personal information they obtained and stored and the foreseeable consequences of a data breach that disclosed customers' personal information, including the fact that those customers owned crypto-assets, to hackers and other third parties.

129. Ledger's and Shopify's violations of Section 5 of the FTC Act (and similar state statutes) constitute negligence per se. This negligence was, at least, a substantial factor in causing the Class members' personal information to be improperly accessed, disclosed, and otherwise compromised, and in causing the Class members' other injuries as a result of the data breaches.

130. The Class members, including Plaintiffs, are within the class of persons that Section 5 of the FTC Act (and similar state statutes) was intended to protect. In addition, the harm that the Class members have suffered is the type of harm that the FTC Act (and similar state statutes) were

intended to prevent. Indeed, the FTC has pursued over fifty enforcement actions against businesses that, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same or similar harm suffered by the Class members.

131. As a direct and proximate result of Ledger's and Shopify's negligence, the Class members have been injured as described herein and are entitled to damages, including compensatory, punitive, and nominal damages, in an amount to be proven at trial.

THIRD CAUSE OF ACTION

DECLARATORY JUDGMENT AND INJUNCTIVE RELIEF

(On Behalf of Plaintiffs, the Nationwide Class, and the Nationwide Phishing Subclass and, Alternatively, on Behalf of the Remaining Non-Consumer Subclasses)

132. Plaintiffs incorporate the preceding paragraphs.

133. Under the Declaratory Judgment Act, 28 U.S.C. § 2201, *et seq.*, this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and grant further necessary relief. The Court also has broad authority to restrain acts, such as here, that are tortious and violate the terms of the federal and state statutes described in this Complaint.

134. An actual controversy has arisen in the wake of the Data Breach regarding Ledger's and Shopify's present and prospective duties to reasonably safeguard customers' and consumers' personal information and whether Ledger and Shopify are maintaining data-security measures adequate to protect the Class members, including Plaintiffs, from further data breaches that compromise their personal information.

135. Plaintiffs allege that Ledger's and Shopify's data-security measures remain inadequate. Ledger and Shopify deny these allegations. In addition, Plaintiffs continue to suffer injury as a result of the compromise of their personal information and remain at imminent risk that further compromises of their personal information will occur in the future.

136. Pursuant to its authority under the Declaratory Judgment Act, Plaintiffs ask the Court to enter a judgment declaring, among other things, the following:

(a) Ledger and Shopify owe a duty to secure consumers' personal information and to timely notify consumers of a data breach under the common law, Section 5 of the FTC Act, and various state statutes; and

(b) Ledger and Shopify are in breach of these legal duties by failing to employ reasonable measures to secure consumers' personal information.

137. Plaintiffs further ask the Court to issue corresponding prospective injunctive relief requiring Ledger and Shopify to employ adequate security protocols consistent with law and industry standards to protect consumers' personal information.

138. If an injunction is not issued, the Class members will suffer irreparable injury, and lack an adequate legal remedy, in the event of another data breach at Ledger and/or Shopify. The risk of another such breach is real, immediate, and substantial. If another breach at Ledger and/or Shopify occurs, the Class members will not have an adequate remedy at law because many of the resulting injuries are not readily quantified and they will be forced to bring multiple lawsuits to rectify the same conduct.

139. The hardship to the Class members if an injunction does not issue exceeds the hardship to Ledger and Shopify if an injunction is issued. Among other things, if another massive data breach occurs at Ledger and/or Shopify, the Class members will likely be subjected to substantial hacking attempts, physical threats, and other damage. On the other hand, the cost to Ledger and Shopify of complying with an injunction by employing reasonable prospective data security measures is relatively minimal, and Ledger and Shopify have pre-existing legal obligations to employ such measures.

140. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing additional data breaches at Ledger and/or Shopify, thus eliminating the additional injuries that would result to the Class members and the millions of consumers whose personal and confidential information would be further compromised.

FOURTH CAUSE OF ACTION

CALIFORNIA UNFAIR COMPETITION LAW

Cal. Bus. & Prof. Code § 17200, *et seq.*

(On Behalf of Plaintiffs, the Nationwide Class, the Nationwide Phishing Subclass, and the Nationwide Consumer Class, and Alternatively, on Behalf of the California Subclass, California Phishing Subclass and California Consumer Class)

141. Plaintiffs incorporate the preceding paragraphs.

142. Ledger and Shopify are "persons" as defined by Cal. Bus. & Prof. Code § 17201.

143. California's Unfair Competition Law (the "UCL") prohibits "unfair competition," which Ledger and Shopify violated by engaging in unlawful, unfair, and deceptive business acts and practices, including the following:

a. Failing to implement and maintain reasonable security measures to protect the California Subclass members' personal information from unauthorized disclosure, release, data breaches, and theft, which was a direct and proximate cause of the Data Breach. Ledger and Shopify failed to identify foreseeable security risks, remediate identified security risks, and adequately improve security following previous cybersecurity incidents. This conduct, with little if any utility, is unfair when weighed against the harm to the California Subclass members whose personal information has been compromised.

b. Ledger's and Shopify's failures to implement and maintain reasonable security measures also were contrary to legislatively declared public policy that seeks to protect consumers' data and ensure that entities that are trusted with it use appropriate security measures. These policies are reflected in laws, including the FTC Act, 15 U.S.C. § 45, and California's Consumer Records Act, Cal. Civ. Code § 1798.81.5.

c. Ledger's and Shopify's failures to implement and maintain reasonable security measures also led to substantial consumer injuries, as described above, that are not outweighed by any countervailing benefits to consumers or competition. Moreover, because consumers could not know of Ledger's and Shopify's inadequate security, consumers could not have reasonably avoided the harms that Ledger and Shopify caused.

d. Engaging in unlawful business practices by violating Cal. Civ. Code § 1798.82.

144. Ledger and Shopify have engaged in "unlawful" business practices by violating multiple laws, including California's Consumer Records Act, Cal. Civ. Code §§ 1798.81.5 (requiring reasonable data security measures) and 1798.82 (requiring timely breach notification);

California's Consumers Legal Remedies Act, Cal. Civ. Code § 1780, *et seq.*; the FTC Act, 15 U.S.C. § 45; and California common law. Ledger's and Shopify's unlawful, unfair, and deceptive acts and practices include the following:

a. Failing to implement and maintain reasonable security and privacy measures to protect the Class members' personal information, including the confidential fact that those individuals had purchased a Ledger and owned crypto-assets, which was a direct and proximate cause of the Data Breach and the Class members' damages;

b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of the Class members' personal information, including the confidential fact that those individuals had purchased a Ledger and owned crypto-assets, including duties imposed by the FTC Act, 15 U.S.C. § 45, which was a direct and proximate cause of the Data Breach;

d. Misrepresenting that they would protect the privacy and confidentiality of the Class members' personal information, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that they would comply with common law and statutory duties pertaining to the security and privacy of the Class members' personal information, including duties imposed by the FTC Act, 15 U.S.C. § 45;

f. Omitting, suppressing, and concealing the material fact that they did not reasonably or adequately secure the Class members' personal information;

g. Omitting, suppressing, and concealing the material fact that they did not comply with common law and statutory duties pertaining to the security and privacy of the Class members' personal information, including duties imposed

by the FTC Act, 15 U.S.C. § 45; and

h. Misrepresenting that Ledger provided the highest level of security for crypto-assets and that Ledger devices and services were worth the amounts paid by the customers, when in reality, Ledger and Shopify permitted the dissemination of personal information to hackers and bad actors, causing Ledger's devices and services to have less actual value or to be worthless.

145. Ledger's and Shopify's representations and omissions were material because they were likely to deceive reasonable consumers about the value of Ledger's and Shopify's services and the adequacy of Ledger's and Shopify's data security, ability to protect the confidentiality of consumers' personal information, and ability to protect the confidentiality of the fact that consumers had purchased a Ledger and/or owned crypto-assets.

146. As a direct and proximate result of Ledger's and Shopify's deceptive and unlawful acts and practices, the Class members are entitled to restitution in an amount to be proven at trial, for, among other things, the loss of the benefit of their bargain with Ledger, as they would not have paid Ledger for goods and services or would have paid less for such goods and services but for Ledger's and Shopify's misconduct.

147. The Class members seek all monetary and non-monetary relief allowed by law, including restitution of all revenues stemming from Ledger's and Shopify's unfair, unlawful, and fraudulent business practices or use of their Personal Information; declaratory relief; reasonable attorneys' fees and costs under California Code of Civil Procedure § 1021.5; injunctive relief; and other appropriate equitable relief.

FIFTH CAUSE OF ACTION

CALIFORNIA CONSUMER LEGAL REMEDIES ACT
Cal. Civ. Code § 1750, *et seq.*
(On Behalf of Plaintiffs, the Nationwide Class, the Nationwide Phishing Subclass, and the Nationwide Consumer Class and, Alternatively on Behalf of the California Subclass, California Phishing Subclass and California Consumer Class)

148. Plaintiffs incorporate the preceding paragraphs.

149. The Consumers Legal Remedies Act, Cal. Civ. Code § 1750, *et seq.* ("CLRA"), is a comprehensive statutory scheme that is to be liberally construed to protect consumers against unfair and deceptive business practices in connection with the conduct of businesses providing goods, property or services to consumers primarily for personal, family, or household use.

150. Ledger and Shopify are "persons" as defined by California Civil Code §§ 1761(c) and 1770, and have provided "services" as defined by California Civil Code §§ 1761(b) and 1770.

151. California Civil Code § 1770(a)(5) prohibits one who is involved in a transaction from "[r]epresenting that goods or services have sponsorship, approval, characteristics, ingredients, uses, benefits, or quantities [which] they do not have[.]"

152. California Civil Code § 1770(a)(7) prohibits one who is involved in a transaction from "[r]epresenting that goods or services are of a particular standard, quality, or grade . . . if they are of another."

153. Class members are "consumers" as defined by California Civil Code §§ 1761(d) and 1770, and have engaged in a "transaction" as defined by California Civil Code §§ 1761(e) and 1770.

154. Ledger's and Shopify's acts and practices were intended to and did result in the sales of products and services to the Class members in violation of California Civil Code § 1770.

155. Ledger's and Shopify's acts and practices were intended to and did result in the sales of products and services to the Class members in violation of California Civil Code § 1770, including, but not limited to, the following:

a. Representing that goods or services have characteristics that they do not have;

b. Representing that goods or services are of a particular standard, quality, or grade when they were not;

c. Advertising goods or services with intent not to sell them as advertised; and

d. Representing that the subject of a transaction has been supplied in accordance with a previous representation when it has not.

156. Ledger's and Shopify's representations and omissions were material because they were likely to and did deceive reasonable consumers about the adequacy of Ledger's and Shopify's data security and ability to protect the confidentiality of consumers' personal information, including the confidentiality of the fact that consumers purchased a Ledger devices or service and, therefore, owned crypto-assets.

157. If Ledger and/or Shopify disclosed to the Class members that their data systems were not secure and, thus, vulnerable to attack, Ledger and Shopify would have been unable to continue in business and would have been forced to adopt reasonable data security measures and comply with the law.

158. Instead, Ledger and Shopify received, maintained, and compiled the Class members' personal information as part of the services Ledger and Shopify provided without advising the Class members that Ledger's and Shopify's data-security practices were insufficient to maintain the safety and confidentiality of the Class members' personal information. Accordingly, the Class members acted reasonably in relying on Ledger's and Shopify's misrepresentations and omissions, the truth of which they could not have discovered.

159. As a direct and proximate result of Ledger's and Shopify's violations of California Civil Code § 1770, the Class members are entitled to injunctive relief. Plaintiffs shall provide the notice required by California Civil Code § 1782(a) and, upon the expiration of the statutory notice and cure period, amend this claim to seek damages, including punitive damages.

160. As set forth above, the Class members will upon amendment seek all monetary and non-monetary relief allowed by law, including damages, an order enjoining the acts and practices described above, attorneys' fees, and costs under the CLRA.

SIXTH CAUSE OF ACTION

GEORGIA UNIFORM DECEPTIVE TRADE PRACTICES ACT

O.C.G.A § 10-1-370, *et seq.*

(On Behalf of the Georgia Subclass, Georgia Phishing Subclass, and Georgia Consumer Subclass)

161. Plaintiffs incorporate the preceding paragraphs.

162. Ledger, Shopify, and the Georgia Subclass members are "persons" within the meaning of § 10-1-371(5) of the Georgia Uniform Deceptive Trade Practices Act ("Georgia UDTPA").

163. Ledger and Shopify engaged in deceptive trade practices in the conduct of its business, in violation of Georgia Code ("O.C.G.A.") § 10-1-372(a), including, but not limited to:

a. Representing that goods or services have characteristics that they do not have;

b. Representing that goods or services are of a particular standard, quality, or grade when they were not;

c. Advertising goods or services with intent not to sell them as advertised; and

d. Representing that the subject of a transaction has been supplied in accordance with a previous representation when it has not.

164. Ledger's and Shopify's deceptive trade practices include, but are not limited to:

a. Failing to implement and maintain reasonable security and privacy measures to protect the Georgia Subclass members' Personal Information, which was a direct and proximate cause of the Data Breach;

b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Georgia Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, the Fair Credit Reporting Act ("FCRA"), 15 U.S.C. § 1681e, and the Gramm-Leach-Bliley Act ("GLBA"), 15 U.S.C. § 6801, *et seq.*, which was a direct and proximate cause of the Data Breach;

d. Misrepresenting that they would protect the privacy and confidentiality of the Georgia Subclass members' Personal Information, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that they would comply with common law and statutory duties pertaining to the security and privacy of the Georgia Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, the FCRA, 15 U.S.C. § 1681e, and the GLBA, 15 U.S.C. § 6801, *et seq.*;

f. Omitting, suppressing, and concealing the material fact that they did not reasonably or adequately secure the Georgia Subclass members' Personal Information; and

g. Omitting, suppressing, and concealing the material fact that they did not comply with common law and statutory duties pertaining to the security and privacy of the Georgia Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, the FCRA, 15 U.S.C. § 1681e, and the GLBA, 15 U.S.C. § 6801, *et seq.*

165. Ledger's and Shopify's representations and omissions were material because they were likely to and did deceive reasonable consumers about the adequacy of Ledger's and Shopify's data security and ability to protect the confidentiality of consumers' personal information, including the confidentiality of the fact that consumers purchased a Ledger devices or service and, therefore, owned crypto-assets.

166. Ledger and Shopify intended to mislead the Georgia Subclass members and induce them to rely on its misrepresentations and omissions.

167. In the course of their businesses, Ledger and Shopify engaged in activities with a tendency or capacity to deceive.

168. Ledger and Shopify acted intentionally, knowingly, and maliciously to violate Georgia's UDTPA, and recklessly disregarded the Georgia Subclass members' rights.

169. If Ledger and/or Shopify disclosed to the Georgia Subclass members that their data systems were not secure and, thus, vulnerable to attack, Ledger and Shopify would have been unable to continue in business and would have been forced to adopt reasonable data security measures and comply with the law.

170. Instead, Ledger and Shopify received, maintained, and compiled the Georgia Subclass members' personal information as part of the services Ledger and Shopify provided

without advising the Georgia Subclass members that Ledger's and Shopify's data-security practices were insufficient to maintain the safety and confidentiality of the Georgia Subclass members' personal information. Accordingly, the Georgia Subclass members acted reasonably in relying on Ledger's and Shopify's misrepresentations and omissions, the truth of which they could not have discovered.

171. As a direct and proximate result of Ledger's and Shopify's deceptive trade practices, the Georgia Subclass members have suffered and will continue to suffer monetary and non-monetary damages, in an amount to be proven at trial, for injuries that include at least the following ascertainable losses of money or property:

a. the loss of the benefit of their bargain with Ledger, as they would not have paid Ledger for goods and services or would have paid less for such goods and services but for Ledger's and Shopify's misconduct;

b. losses from fraud and theft;

c. costs for credit monitoring, identity protection services, or other services or products to attempt to recover stolen crypto-assets, protect crypto-assets, or protect personal information;

d. time and expenses incurred and to be incurred in monitoring their financial accounts for fraudulent activity;

e. time and money spent attempting to recover stolen crypto-assets, protect crypto-assets, or protect personal information;

f. loss of value of their personal information;

g. time and money spent attempting to replace or replacing the hardware and services that Ledger was supposed to provide but failed to provide; and

h. an increased, imminent risk of fraud and identity theft.

172. The Georgia Subclass members seek all relief allowed by law, including injunctive relief, and reasonable attorneys' fees and costs, under O.C.G.A. § 10-1-373.

PRAYER FOR RELIEF

On behalf of themselves, the Class, and the Subclasses, Plaintiffs request as follows:

(a) That the Court determines that this Action may be maintained as a Class Action, that Plaintiffs be named as Class Representatives of the Class, that the undersigned be named as Lead Class Counsel of the Class, and directs that notice of this Action be given to Class members;

(b) That the Court enter an order declaring that Defendants' actions, as set forth in this Complaint, violate the laws set forth above;

(c) That the Court award Plaintiffs and the Class damages in an amount to be determined at trial;

(d) That the Court issue appropriate equitable and any other relief against Defendants to which Plaintiffs and the Class are entitled, including but not limited to an Order requiring Defendants to cooperate and financially support civil and/or criminal asset recovery efforts;

(e) That the Court award Plaintiffs and the Class pre- and post-judgment interest (including pursuant to statutory rates of interest set under State law);

(f) That the Court award Plaintiffs and the Class their reasonable attorneys' fees and costs of suit; and

(g) That the Court award any and all other such relief as the Court may deem just and proper under the circumstances.

JURY TRIAL

Pursuant to Federal Rule of Civil Procedure 38(b), Plaintiffs respectfully demand a trial by jury for all claims.

Dated: April 6, 2021

Respectfully submitted,

/s/ Todd M. Scheider

Todd M. Schneider (SBN 158253)
Jason H. Kim (SBN 220279)
Matthew S. Weiler (SBN 236052)
Kyle G. Bates (SBN 299114)
SCHNEIDER WALLACE
COTTRELL KONECKY LLP
2000 Powell Street, Suite 1400
Emeryville, California 94608
Telephone: (415) 421-7100
Email: tschneider@schneiderwallace.com
Email: jkim@schneiderwallace.com
Email: mweiler@schneiderwallace.com
Email: kbates@schneiderwallace.com

/s/ Kyle W. Roche

Kyle W. Roche (*pro hac vice application forthcoming*)
Richard Cipolla (*pro hac vice application forthcoming*)
Jolie Huang (*pro hac vice application forthcoming*)
ROCHE FREEDMAN LLP
99 Park Avenue, 19th Floor
New York, NY 10016
Telephone: (646) 970-7509
Email: kyle@rcfllp.com
Email: rcipolla@rcfllp.com
Email: jhuang@rcfllp.com

Velvel Freedman (*pro hac vice application forthcoming*)
Constantine P. Economides (*pro hac vice application forthcoming*)
ROCHE FREEDMAN LLP
200 South Biscayne Boulevard
Miami, FL 33131
Telephone: (305) 971-5943
Email: vel@rcfllp.com
Email: ceconomides@rcfllp.com

Counsel for Plaintiffs