IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF DELAWARE

GREGORY FORSBERG, CHRISTOPHER GUNTER, SAMUEL KISSINGER, AND SCOTT SIPPRELL, individually and on behalf of all others similarly situated,

Plaintiffs,

v.

SHOPIFY, INC., SHOPIFY HOLDINGS (USA), INC., SHOPIFY (USA) INC., AND TASKUS, INC.

Defendants.

Case No.:

JURY TRIAL DEMANDED

CLASS ACTION COMPLAINT

Individually and on behalf of others similarly situated, Plaintiffs Gregory Forsberg ("Mr. Forsberg"), Christopher Gunter ("Mr. Gunter"), Samuel Kissinger ("Mr. Kissinger), and Scott Sipprell ("Mr. Sipprell") (collectively, "Plaintiffs"), bring this action against Defendants Shopify, Inc., Shopify Holdings (USA), Inc., Shopify (USA) Inc. (collectively, "Shopify"), and TaskUs, Inc. ("TaskUs") (collectively, the "Defendants"). 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 for the allegations set forth herein exists and will be revealed after a reasonable opportunity for discovery.

I. INTRODUCTION

1. This is a class action for damages against TaskUs and Shopify for their failure to exercise reasonable care in securing and safeguarding consumer information in connection with a massive 2020 data breach impacting Ledger SAS ("Ledger") cryptocurrency hardware wallets ("Ledger Wallets"), resulting in the unauthorized public release of approximately 272,000 pieces of detailed personally identifiable information ("PII"), including Plaintiffs' and "Class" (defined below) members' full names, email addresses, postal addresses, and telephone numbers.

2. Ledger sells Ledger Wallets through its e-commerce website, which is run on Shopify's platform.

3. Ledger Wallets store the "private keys" of an individual's crypto-assets. These private keys are similar to bank account passwords in that access to the private keys allows an individual to transfer the assets out of a cryptocurrency account. Unlike a bank account transaction, however, cryptocurrency transactions are non-reversible—once assets are transferred out of a cryptocurrency account, they are able to be distributed or spent with little information about where they could have gone.

4. Ledger Wallets were marketed as providing owners of cryptocurrency with the best security for their cryptocurrency because they hold password information in a physical form and restrict transfer of crypto-assets in an individual's account unless the physical device is mounted to a computer and a twenty-four-word passphrase is entered.

5. Because of these features, Ledger's platform is built on marketing the utmost security and trust to its customers. Ledger and Shopify know that cryptocurrency transactions are publicly visible through a transaction's underlying blockchain, but cannot be traced back to their particular owner without more information. When hackers know the identity of a

cryptocurrency owner and know what platform that consumer is storing their crypto-assets on, the hacker can work backwards to create a targeted attack aimed at luring hardware wallet owners into mounting their hardware device to a computer and entering their passphrase, allowing unfettered access and transfer authority over their crypto-assets.

6. Accordingly, to the world of cybercriminals, Ledger's customer list, which was in the possession of Shopify at the time of the "Data Breach" (defined below), is extremely valuable. By accessing Ledger customer PII entrusted to Shopify, such as full names, email addresses, postal addresses, and telephone numbers, hackers can engineer targeted communications—known as phishing attacks—that compel users to unlock their cryptocurrency accounts and make untraceable, irreversible transfers of cryptocurrency into these criminals' accounts overseas and within the United States. The security of Ledger customers' PII is accordingly of the utmost importance. One instance of a customer mistakenly releasing their account information to hackers can lead to the loss of millions of dollars in cryptocurrency that will never be returned to their owner.

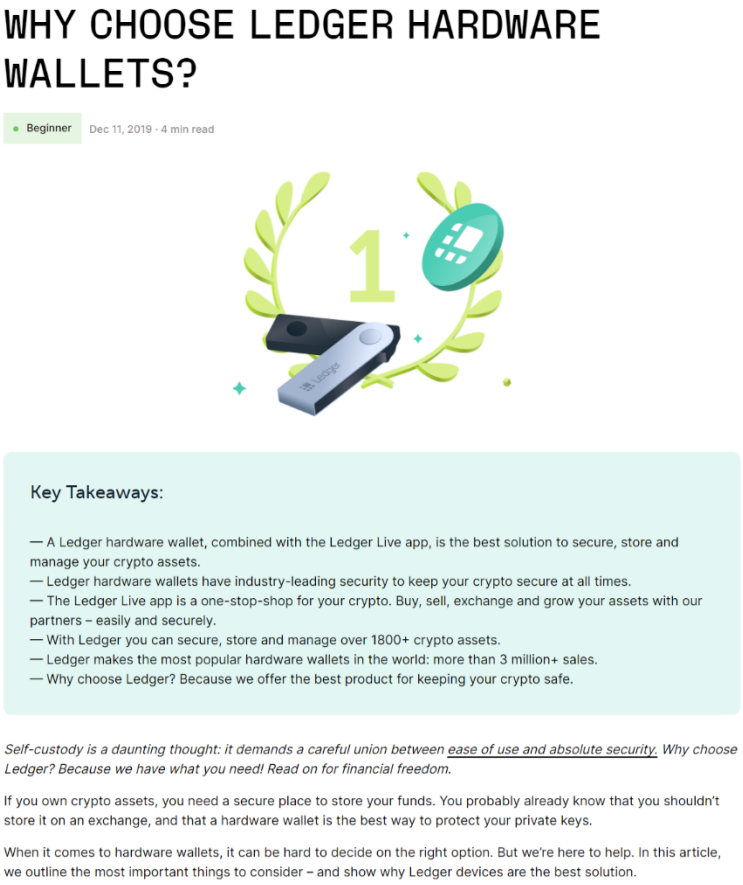
7. With their PII in hackers' hands, Plaintiffs and Class members are no longer in possession of a secure cryptocurrency portfolio.

8. Ledger and Shopify understand the seriousness of the misuse of customers' PII, and purport to address these issues. For example, Ledger advertises that it has "the highest security standards," and that it "continuously look[s] for vulnerabilities on Ledger products as well as [its] providers' products in an effort to analyze and improve the security," and that its products provide "the highest level of security for crypto assets."[1] Shopify touts that it "work[s]

[1] *The Ledger Donjon*, LEDGER (Oct. 23, 2019), https://www.ledger.com/academy/security/the-ledger-donjon (last accessed Feb. 22, 2022).

tirelessly to protect your information, and to ensure the security and integrity of our platform."[2]

9. Ledger has built a reputation of maintaining the highest trust possible with its customers, including those related to consumer PII that the company shares with third parties



WHY CHOOSE LEDGER HARDWARE WALLETS?

Beginner Dec 11, 2019 · 4 min read

Key Takeaways:

— A Ledger hardware wallet, combined with the Ledger Live app, is the best solution to secure, store and manage your crypto assets.
— Ledger hardware wallets have industry-leading security to keep your crypto secure at all times.
— The Ledger Live app is a one-stop-shop for your crypto. Buy, sell, exchange and grow your assets with our partners – easily and securely.
— With Ledger you can secure, store and manage over 1800+ crypto assets.
— Ledger makes the most popular hardware wallets in the world: more than 3 million+ sales.
— Why choose Ledger? Because we offer the best product for keeping your crypto safe.

Self-custody is a daunting thought: it demands a careful union between ease of use and absolute security. Why choose Ledger? Because we have what you need! Read on for financial freedom.

If you own crypto assets, you need a secure place to store your funds. You probably already know that you shouldn't store it on an exchange, and that a hardware wallet is the best way to protect your private keys.

When it comes to hardware wallets, it can be hard to decide on the right option. But we're here to help. In this article, we outline the most important things to consider – and show why Ledger devices are the best solution.

like Shopify. Below are true and correct screenshots of Ledger's advertising claims on its website, as well as the company's policies related to the information that it shares with third parties in the course of its business:

[2] *Privacy Policy*, SHOPIFY (Jan. 10, 2022), https://www.shopify.com/legal/privacy#information-protection (last accessed Feb. 22, 2022).

WHY IS LEDGER NANO SO SECURE?

Beginner Jan 14, 2021 - 3 min read

Key Takeaways:

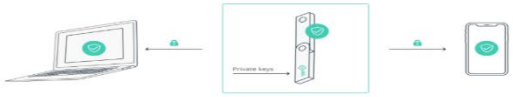
— Your crypto assets are completely intangible and exist solely on the blockchain
— How your handle your private keys for assets on the blockchain will define how secure those assets are
— Ledger hardware wallets allow you to store your keys within a device that is protected by Secure Element – a military grade security chip. Each device generates its own, unique 24-word recovery phrase which can be used to recover your associated funds if the device itself is lost
— Ledger hardware wallets allow users to set a PIN code, so that nobody else can use the device to access your assets, even if it is lost or stolen

Back in our "Own and use it" Playlist, we explained how important it is to be the true owner of your funds, by ensuring the security and ownership of your private keys. That's where our Nano hardware wallets come in. But just why is Ledger Nano so secure? Here, we explain.

A DEVICE THAT GIVES YOU FULL OWNERSHIP OVER YOUR CRYPTO

Two things really matter when you invest in crypto: security and ownership of your coins. As previously mentioned, crypto assets are digital data stored on the blockchain, they are nowhere physically speaking. This means that it is on you to ensure they remain truly and safely yours. To do so, you need to protect the private key which gives access to your coins.

At Ledger, we offer you the best security and provide you with ownership and control over your assets. Therefore, we created the Nano hardware wallets combined with one-single app Ledger Live, to safeguard your private keys and mitigate potential risks. In short, the devices are designed so that your private keys never leave the security of the hardware, even when connecting your wallet to your smartphone or desktop.



WHY IS LEDGER NANO SO SECURE: DON'T TRUST, VERIFY

At Ledger, we are pioneering hardware wallet technology that provides unprecedented levels of security for crypto assets. How? By creating certified devices that are secure by design.

- All of our Nano hardware wallets possess a certified chip, designed to withstand sophisticated attacks. They are called Secure Element (SE), and are cryptographically protected, similar to the ones used in the likes of passports and SIM cards. Unlike the generic chips used in remote controls or microwaves, your private keys stay safe and isolated inside the Secure Element chips.
- Besides, Ledger Nano wallets are the only hardware wallets to have their own custom OS – called BOLOS. One designed specifically to protect your crypto assets. Not your family pictures. A tailor-made OS provides you with an enhanced security.
- Need more proof? Ledger Nano wallets are the first and only certified hardware wallets on the market, certified by ANSSI, the French independent cyber security agency.

MAKE YOUR DEVICE SECURELY YOURS: THE 24-WORD PHRASE

Every hardware wallet comes with an authentication process. One that commonly operates at two different levels: the PIN number and the Recovery phrase.

YOUR PIN NUMBER OR PIN CODE

When setting up a new Nano device, you are asked to choose a PIN code. This code allows you to unlock your device, similarly to the passcode you use to unlock your smartphone. Here is a list of *DOs* and *DONTs* to help kick it off.

YOUR 24-WORD RECOVERY PHRASE

You may have already heard about that one. Whether it's called Recovery Phrase, Seed Phrase, 24 Words, it's all the same. Your 24-word recovery phrase is the only backup to your private keys.

While your PIN code is unique to your physical device, your Recovery phrase is directly linked to your private key, therefore to your funds. It remains the same even when you switch to another device. And if discovered by anyone, it would give them access to your funds.

Your recovery phrase is a unique sequence of 24 words, randomly generated by your hardware wallet during initialization This is the only time they are displayed and they are the only backup to your funds. Since no third parties are involved, there is no other backup. You are the only one in charge of your money.

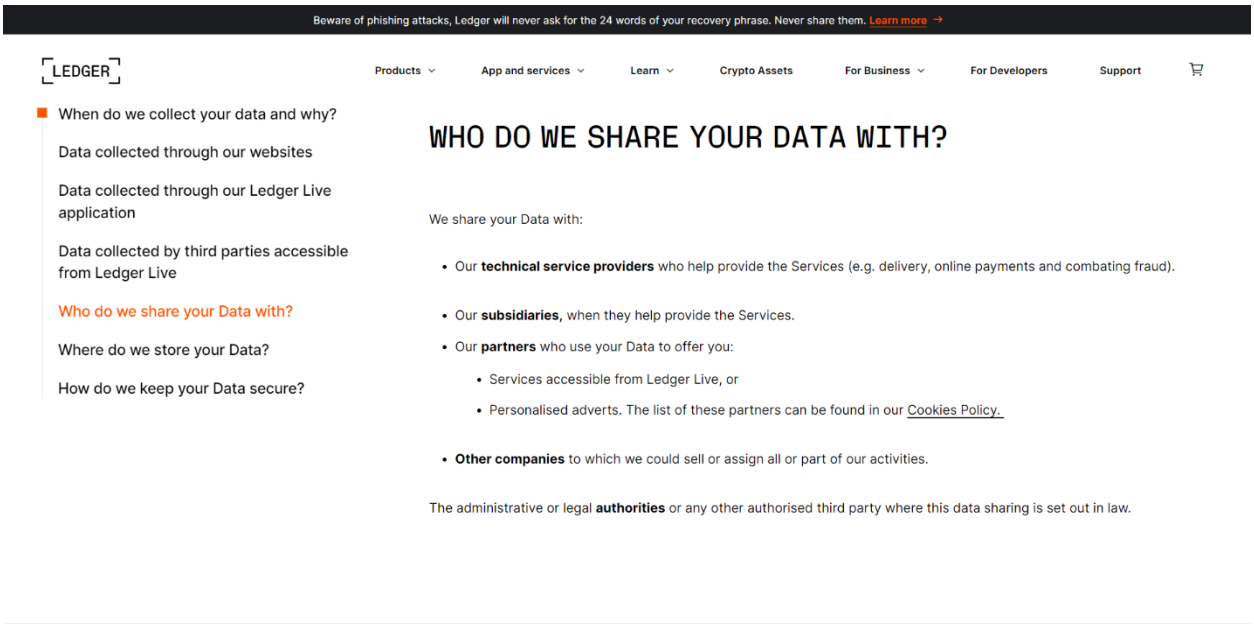
For example, if you forget your PIN code or lose your device, your 24 words allow you to regain access to your funds via your backup Ledger hardware wallet or simply any other wallet.

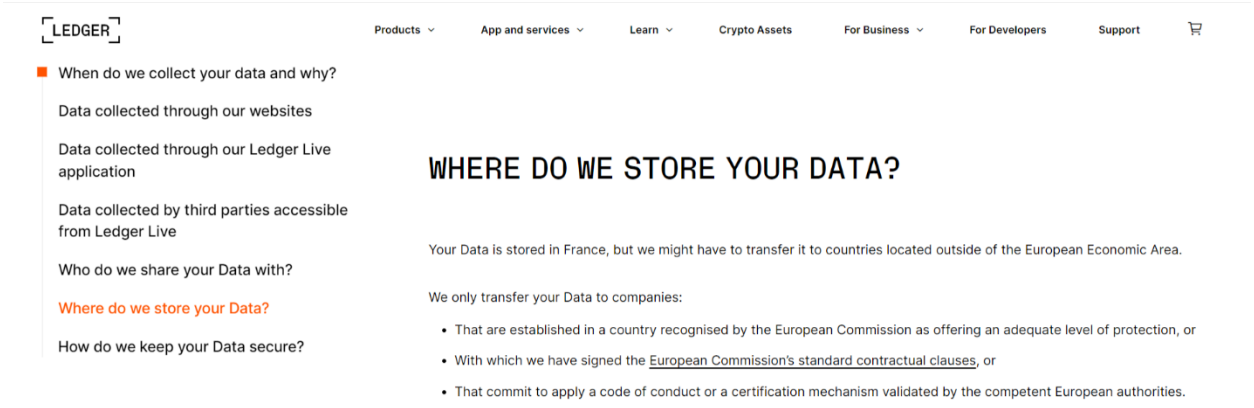
Conclusion: do not share or lose your 24 words, ever. Keep them safe and secure.

How? When your 24 words are displayed on your device screen, you must carefully write down (in the correct order and without any misspellings) your 24 words. Then safeguard them after you initialize your hardware wallet. To help you do that, every Ledger hardware wallet comes with a Recovery Sheet: a physical card specifically designed to store your 24 words. Please review the best practices to protect your recovery phrase and sheet, and carefully follow them. Once again, it is your responsibility.

DATA COLLECTED THROUGH OUR WEBSITES

User action	Data collected	Data usage	Reason for processing (legal basis)	Retention period
Purchase of a Ledger product	Name, email address, delivery and billing address, phone number, company name, intra-community VAT number, product bought, delivery method and payment, order amount, currency	Processing orders, invoices and payments, delivery, analytics, preventing fraud, managing complaints and sending notifications	Performance of the contract you agreed with Ledger upon buying one of our products	Active database: 3 months from delivery of the product Archive: 10 years (tax and accounting obligations)
Request to receive marketing emails (including our newsletter)	Email address, campaign number, logs	Sending emails on our latest developments, promotions and customer surveys	Consent to receive marketing emails	3 years from the request
Request sent to customer services (on the dedicated platform or through social media)	Name, email and postal address, telephone number (for product exchanges), Handle used on social media, content of our exchanges, identification document (if verification is necessary)	Processing the request, quality control, verifying information is correct and preventing fraud	Ledger's legitimate interest	5 years from the request
Browsing our websites Please note: We collect your Browsing Data using various technologies such as cookies (for more information, please visit our Cookies Policy).	Consent or refusal to save cookies on your device	Cookies are saved (or not saved) on the device	Legitimate interest	6 months from the user's decision
	IP address, operating system, browser, devices used, date and time of visit, URLs of clickstream to, through and from our website, products viewed and searched, download errors, duration of visit on certain pages, interaction between pages	Bug-fixing, analytics, combating fraud, personalising your experience, displaying adverts on third-party websites	Dependent on the purpose of the cookies saved: - Legitimate interest for technical cookies - Consent for functional, performance and advertising cookies	The time needed to fulfil the purpose of the cookies saved (for example, one session for session cookies)
Participation in customer surveys	Name, age, email address, family situation, profession, country, product opinion, comments	Carrying out marketing studies, improving our products and services	Legitimate interest	6 months from the end of the survey
Participating in our referral programme	Name, email address and IP address of referrers and referral recipients, password of referrer, purchase amount of referral recipients	Managing the programme, sending emails (referral offers, purchase made by referral recipients, attributing rewards)	Performance of the contract you agreed with Ledger by participating in the programme	For as long as the referrer is a member of the programme, except in the event of prolonged
Request to be re-contacted on the subject of our B2B products	Name, company, role, email address, telephone number, country	Making contact, sending emails on our latest developments, promotions and customer surveys	Legitimate interest	5 years from the request
Signing up to our affiliate programme	Name, email address, company, BTC address, identity document, intra-community VAT number and proof of residence (where required).	Managing the programme, sending emails on the programme's latest developments, remuneration	Performance of the contract you agreed with Ledger when signing up to the programme	For as long as the affiliate is a member of the programme, except in the event of prolonged inactivity





10. Despite the repeated promises and world-wide advertising campaign touting unmatched security for its customers, Ledger—and its data processing vendors, Shopify and TaskUs—repeatedly and profoundly failed to protect its customers' identities, causing targeted attacks on thousands of customers' crypto-assets and causing Class members to receive far less security than they thought they had purchased with their Ledger Wallets.

11. Between April and June of 2020, hackers gained access to and exploited a Ledger database vulnerability through its e-commerce vendor, Shopify, and TaskUs as a third-party contractor, in order to obtain a list of Ledger's customers' PII (the "Data Breach"). By June of 2020, hundreds of thousands of victims' information had been traded on the black market, leaving Plaintiffs and Class members vulnerable to multiple phishing attacks.

12. The known extent of the Data Breach became much worse over subsequent months. Between June and December of 2020, the hackers who had acquired the Ledger customer list from Shopify (due to Shopify and TaskUs negligence) had published the data online, providing over 270,000 names, email addresses, physical addresses, phone numbers, and other customer information to every hacker who wanted access to this information. The attacks on Ledger customers, targeted at obtaining their confidential wallet passphrases or forcing customers to transfer thousands of dollars in cryptocurrency to untraceable accounts across the world, increased exponentially. Customers lost money in phishing attacks and faced threats of physical violence or blackmail if they did not transfer crypto-assets to criminals around the world. Using the customer shipping addresses that Shopify and TaskUs failed to protect, hackers threatened to enter Ledger customers' homes and assault them if they did not provide payment; some cybercriminals even sent targeted phishing attacks under the guise of Ledger customer service representatives, luring Data Breach victims to provide confidential passphrases to hackers and allowing their assets to be drained from their accounts.[3]

13. In the face of these circumstances, rather than acting to protect customer information, Ledger, Shopify, and TaskUs did not even inform Plaintiffs and Class members of

[3] Tim Copeland, *Ledger Won't Reimburse Users After Major Data Attack*, DECRYPT (Dec. 21, 2020), https://decrypt.co/52215/ledger-wont-reimburse-users-after-major-data-hack

the Data Breach. Instead, Ledger initially denied that any compromise of the PII had occurred and continued to claim its products were superior because they provided the best protection for crypto-asset protection.

14. By December 23, 2020, however, Ledger could no longer cover up the Data Breach. The hacked customer list had been posted publicly online and had become widely available.

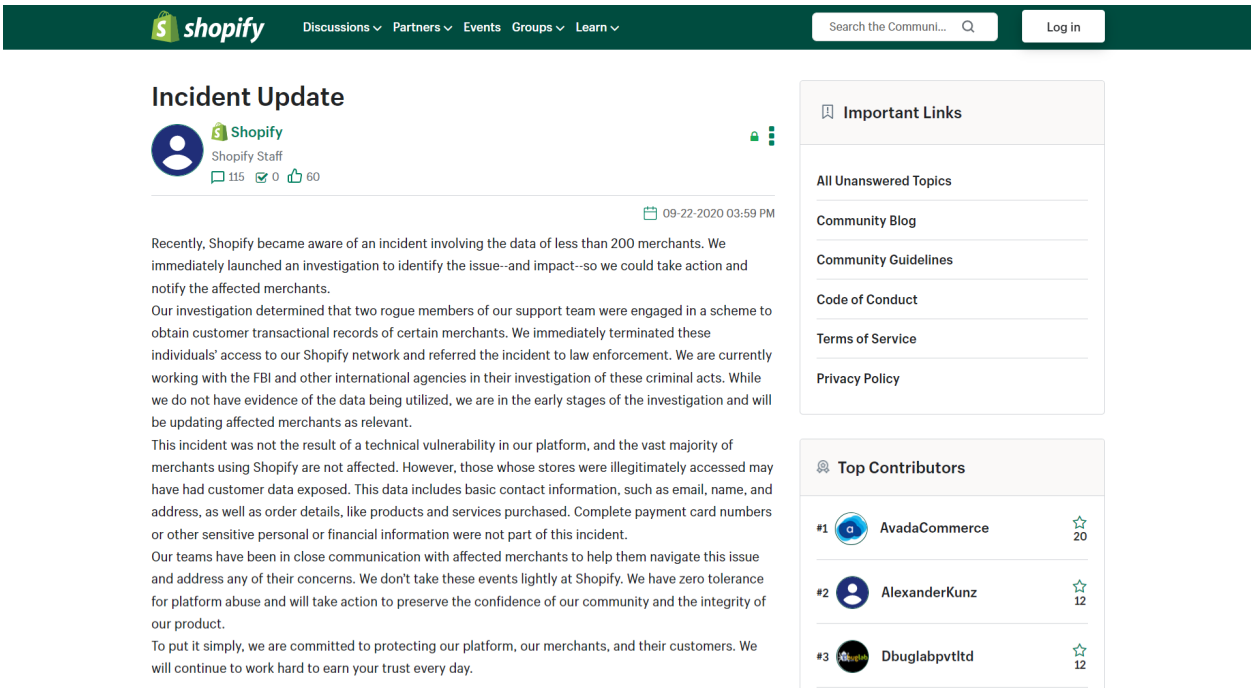
15. In response to this now-public reality, Ledger sent some customers affected by the Shopify and TaskUs Data Breach an email notifying them for the first time that their information had been affected as the result of a breach of Shopify's merchant database; however, the email notice provided nothing more than a passing reference to the Shopify incident further detailed herein.

16. Below is a true and correct recitation of the notification email sent to Ledger customers affected by the Data Breach:

> Dear client,
>
> On December 23, 2020, Shopify, our e-commerce service provider, informed Ledger of an incident involving merchant data. Rogue agent(s) of their customer support team obtained Ledger customer transactional records in April and June 2020. This is related to the incident reported by Shopify in September 2020, which concerns more than 200 merchants, but until December 21, 2020, Shopify had not identified this affected Ledger as well.
>
> We were able to examine the stolen data together with a third party forensic firm to identify the impacted customers.
>
> We regret to inform you that you are part of the customers whose detailed personal information was stolen by Shopify rogue agent(s). Specifically, your name and surname, detail of product(s) ordered, phone number and your postal address were exposed.
>
> We notified the French Data Protection Authority on December 26, 2020. We are continuing to work with Shopify and law enforcement

> on the case; an investigation is already underway, led by the FBI and the RCMP. Ledger also reported the events to the French Public Prosecutor and filed a complaint against the rogue agent(s).
>
> Thefts and attacks such as this cannot go uninvestigated or unprosecuted. We continue to work with law enforcement as well as private investigators on these cases, and we are adding more firepower by hiring additional private investigation capacity, adding experience and approaches to finding those responsible for these data thefts.
>
> FINALLY, keeping you secure is our reason for existing. We will soon release a technical solution that will remove the 24 words as the single pillar of the security of our hardware wallets and will open the door to funds insurance.
>
> If you would like more detail on the many steps we are taking to prevent such incidents in the future, please read this blog post.
>
> Sincerely,
> Pascal Gauthier
> Ledger CEO

17. The notification email provided nothing more than a passing reference to the Shopify and TaskUs Data Breach, with the message containing a single hyperlink to a blog post on Shopify's website from September of 2020 that describes the extent of the Data Breach. A true and correct screenshot of the blog post on Shopify's website is copied below:



18. It would not be revealed until months later that the "rogue members" of Shopify's support team included employees of TaskUs, Inc., a Delaware company that operates as a data vendor for a number of Shopify clients. Also revealed was that a hacker known as "Pokeball" solicited members of TaskUs who processed Shopify merchant data for a list of customers using various merchants' services, including Ledger.[4]

19. Defendants' misconduct, including but not limited to their failure to (a) prevent the Data Breach and (b) take action in response thereto for approximately six months—if not longer—has made targets of Plaintiffs and Class members, with their identities known or available to every hacker in the world who wants access to this information.

20. Defendants' deficient response compounded the harm that has already been experienced by Plaintiffs and Class members. For example, by failing to notify every affected

[4] Natalie Wong & Gerrit De Vynck, *Shopify Says 'Rogue' Employees Stole Data from Merchants*, BLOOMBERG LAW (Sept. 22, 2020), https://news.bloomberglaw.com/privacy-and-data-security/shopify-says-rogue-employees-stole-data-from-merchants?context=article-related.

customer or admit to the full scope of the Data Breach, Shopify and TaskUs left Plaintiffs and Class members unaware of the Data Breach and concomitant hacking risks. The direct result of Defendants' failure to adequately warn their merchant clients of the Data Breach is many Ledger customers falling victim to hackers' phishing emails and resulting fraud.

21. Moreover, Shopify's deficient response to the Data Breach included a failure to provide any support for merchant clients, like Ledger, whose customers had been targeted in the incident, as well as negligently entrusting Ledger customer information to TaskUs's data processing team who, in turn, failed to maintain the information using adequate data safety standards.

22. Shopify is therefore responsible for the actions of TaskUs in its maintenance (or failure to maintain) Plaintiffs' and Class members' PII.

23. TaskUs, who upon information and belief brokered the contract with Shopify to process Shopify data through TaskUS offices located in the United States, also failed to properly maintain Plaintiffs' and Class members' highly sensitive PII, which it knew would lead to targeted cyberattacks resulting in thousands of victims losing cryptocurrency funds that they expected would be kept secure.

24. Had Plaintiffs and Class members known that the information necessary to perform targeted phishing attacks against them would not be adequately protected by Shopify and TaskUs, they would not have paid the amount of money they did to purchase the Ledger Wallets. Nor, for that matter, would they have agreed to have their data transmitted to either company in order to perform e-commerce support for Ledger's operations.

25. On behalf of the Class and several Subclasses of victims impacted by the Data Breach described herein, Plaintiffs seek, under state common law and consumer-protection

statutes, to redress Defendants' misconduct occurring from April 1, 2020 to the present (the "Class Period").

II. PARTIES

A. Plaintiff Gregory Forsberg

26. Plaintiff Forsberg is a citizen of Arizona and resides in Tucson, Arizona. Mr. Forsberg purchased a Ledger Nano S for use as a cryptocurrency wallet to control his cryptocurrency assets. On or around April of 2019, Mr. Forsberg saw advertisements online for Ledger services and hardware. Relying on these representations, Mr. Forsberg purchased the Ledger Nano device from an online retailer and transferred his cryptocurrency assets to his Ledger device. In adding cryptocurrency to his Ledger Wallet, he was required to provide his PII to Ledger's online service, including the types of PII mentioned above in the "Data Collected Through Our Websites" section, including his first and last name, email address, telephone number, and postal address. In making his purchase decision, Mr. Forsberg relied upon the data security services advertised by Ledger, including the company's use of third parties and independent contractors such as Shopify and TaskUs to process customer PII. Mr. Forsberg would not have purchased the Ledger Nano S device had he known that the sensitive information collected by Ledger would be at risk because of the negligence of Defendants, to whom Ledger entrusted Mr. Forsberg's PII. Mr. Forsberg has suffered damages described below, including but not limited to the fraudulent removal of cryptocurrency from his portfolio due to a sophisticated scam attack on his Ledger wallet, and remains at a significant risk of additional attacks now that his PII has been leaked online.

B. Plaintiff Christopher Gunter

27. Plaintiff Gunter is a citizen of North Carolina and resides in Asheville, North Carolina. Mr. Gunter purchased a Ledger Nano S device for use as a cryptocurrency wallet to control his cryptocurrency assets. On or around January of 2018, Mr. Gunter saw advertisements online for Ledger's services and hardware. Relying on these representations, Mr. Gunter purchased the Ledger Nano S device from an authorized reseller on eBay and transferred his cryptocurrency assets from an online Coinbase wallet to the Ledger device using Ledger's online platform in November of 2018. In making the transfer of his cryptocurrency assets from his Coinbase account to his Ledger device, he was required to provide his PII to Ledger's online service, including the types of PII mentioned above in the "Data Collected Through Our Websites" section, including his first and last name, email address, telephone number, and postal address. In making his purchase decision, Mr. Gunter relied upon the data security services advertised by Ledger, including the company's use of third parties and independent contractors such as Shopify and TaskUs to process customer PII. Mr. Gunter would not have purchased the Ledger Nano S had he known that the sensitive information collected by Ledger would be at risk because of the negligence of Defendants, to whom Ledger entrusted Mr. Gunter's PII. Mr. Gunter has suffered damages described below, including but not limited to the fraudulent removal of cryptocurrency from his portfolio due to a sophisticated scam attack on his Ledger wallet, and remains at a significant risk of additional attacks now that his PII has been leaked online.

C. Plaintiff Samuel Kissinger

28. Plaintiff Kissinger is a citizen of Kentucky and resides in Burlington, Kentucky. Mr. Kissinger purchased two Ledger Nano S devices, a Ledger Nano X, and a Ledger Blue for

use as cryptocurrency wallets to control his cryptocurrency assets. On or around August of 2017 and again in October of 2018 when Mr. Kissinger purchased the devices he saw advertisements online for Ledger services and hardware. Relying on these representations, Mr. Kissinger purchased the Ledger Nano device from an online retailer and transferred his cryptocurrency assets to his Ledger device. In adding cryptocurrency to his Ledger Wallet, he was required to provide his PII to Ledger's online service, including the types of PII mentioned above in the "Data Collected Through Our Websites" section, including his first and last name, email address, telephone number, and postal address. In making his purchase decision, Mr. Kissinger relied upon the data security services advertised by Ledger, including the company's use of third parties and independent contractors such as Shopify and TaskUs to process customer PII. Mr. Kissinger would not have purchased the Ledger Nano device had he known that the sensitive information collected by Ledger would be at risk because of the negligence of Defendants, to whom Ledger entrusted Mr. Kissinger's PII. Mr. Kissinger has suffered damages described below, including but not limited to the fraudulent removal of cryptocurrency from his portfolio due to a sophisticated scam attack on his Ledger wallet, and remains at a significant risk of additional attacks now that his PII has been leaked online.

D. Plaintiff Scott Sipprell

29. Plaintiff Sipprell is a citizen of Florida and resides in Saint Augustine, Florida. Mr. Sipprell purchased a Ledger Nano S device for approximately $100 on or around December of 2017 for use as a cryptocurrency wallet to control his cryptocurrency assets. On or around December of 2017, Mr. Sipprell saw advertisements online for Ledger services and hardware. Relying on these representations, Mr. Sipprell purchased the Ledger Nano device from an online retailer while in Woodby Island, Washington and transferred his cryptocurrency assets to his

Ledger device. In adding cryptocurrency to his Ledger Wallet, he was required to provide his PII to Ledger's online service, including the types of PII mentioned above in the "Data Collected Through Our Websites" section, including his first and last name, email address, telephone number, and postal address. In making his purchase decision, Mr. Sipprell relied upon the data security services advertised by Ledger, including the company's use of third parties and independent contractors such as Shopify and TaskUs to process customer PII. Mr. Sipprell would not have purchased the Ledger Nano device had he known that the sensitive information collected by Ledger would be at risk because of the negligence of Defendants, to whom Ledger entrusted Mr. Sipprell's PII. Mr. Sipprell has suffered damages described below, including but not limited to the fraudulent removal of cryptocurrency from his portfolio due to a sophisticated scam attack on his Ledger wallet, and remains at a significant risk of additional attacks now that his PII has been leaked online.

E. Defendant TaskUs, Inc.

30. Defendant TaskUs, Inc. is a Delaware corporation with its principal place of business registered at 1650 Independence Drive, Suite 100, New Braunfels, Texas 78132. TaskUs had access to Ledger customers' PII and failed to secure the received PII or implement any security measures or even screening procedures to ensure that its agents, support representatives, and other individuals to whom Ledger and Shopify entrusted the Private PII data would ensure secure handling of the data.

F. Defendant Shopify, Inc.

31. Defendant Shopify, Inc. is a Canadian Corporation with offices at 151 O'Connor Street, Ground Floor, Ottowa, Ontario K2P 2L8.

G. Defendant Shopify Holdings (USA), Inc.

32. Defendant Shopify Holdings (USA), Inc. is a Delaware corporation with its principal place of business in the United States. Shopify Holdings (USA), Inc. acts as a holding company for all of Shopify Inc.'s US-based subsidiaries.

H. Defendant Shopify (USA) Inc.

33. Defendant Shopify (USA) Inc. is a Delaware corporation with its principal place of business in Ottowa, Canada. It is a wholly owned subsidiary of Shopify, Inc. The Shopify entities had access to Ledger customers' PII and failed to secure the received PII or implement any security measures or even screening procedures to ensure that its agents, support representatives, and other individuals to whom Shopify entrusted the private PII data would ensure secure handling of the data.

34. Upon information and belief, Shopify (USA) Inc. and Shopify Holdings (USA), Inc. are the functional equivalents of Shopify, Inc. because the two entities make no distinction between themselves in the public eye and use the same logos, trademarks, and websites, making it impossible to know the extent of any of the Shopify entities' involvement in this Data Breach.

III. JURISDICTION AND VENUE

35. 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 different state from any defendant.

36. This Court has personal jurisdiction over this action because Defendants Shopify (USA) Inc., Shopify Holdings (USA), Inc., and TaskUs, Inc. are Delaware corporations.

37. Venue is proper in this District under 28 U.S.C. § 1391(b)(1) because Defendants Shopify (USA) Inc., Shopify Holdings (USA), Inc., and TaskUs, Inc. reside within this District.

38. Plaintiffs are informed and believe, and thereon allege, that each and every one of the acts and omissions alleged herein were performed by, and/or attributable to, Defendants.

39. Shopify, Inc. dominates and controls Shopify (USA) Inc.'s and Shopify Holdings (USA)'s internal affairs and daily operations. Not only is Shopify (USA) Inc. a wholly owned subsidiary of Shopify Holdings, which in turn is a wholly owned subsidiary of Shopify, Inc., but there is also a substantial overlap among these entities' executives, thereby imputing Shopify (USA) Inc.'s and Shopify Holdings' jurisdictional contacts with this Court to Shopify, Inc. Indeed, Shopify (USA)'s CEO and CFO is Amy Shapero—the CFO of Shopify, Inc. The Secretary of Shopify (USA) is Shopify Inc.'s Chief Legal Officer. Furthermore, Shopify's job listings note that the company will "hire you [ ] anywhere" as long as it has an "entity where you are." Shopify, therefore, does not differentiate between its entities for any job responsibilities and thus does substantial business through the American employees it hires through its subsidiary companies operating as Delaware corporations, including Shopify (USA) Inc. and Shopify Holdings (USA), Inc.

40. This Court also has personal jurisdiction over Shopify (USA) Inc., Shopify Holdings, and Shopify, Inc. because they solicit customers and transact business in Delaware and throughout the United States, including with Ledger and TaskUs.

IV. FACTUAL ALLEGATIONS

A. Cryptocurrency Generally

41. Cryptocurrency is a digital asset designed to work as a medium of exchange or a store of value. Cryptocurrencies use a variety of cryptographic principles to secure transactions,

control the creation of additional units of currency, and verify the transfer of the underlying digital assets.

42. Bitcoin was the world's first decentralized cryptocurrency. It is also the largest and most popular cryptocurrency, with a market capitalization of approximately $1.08 Billion. Bitcoin's economic market led to a market of other cryptocurrencies that have a market capitalization of approximately $2 Trillion.

43. Underlying every owner of cryptocurrency's assets are records of addresses and transfer amount that track the ownership and transfer of every cryptocurrency in existence. This record is also known as the blockchain, and is completely public, albeit without PII included in this publicly available information.

44. A website known as coinmarketcap.com, which tracks cryptocurrency markets, notes that there are currently more than 17,645 cryptocurrencies in existence.

B. Cryptocurrency Transactions

45. Because information about the transfer of cryptocurrencies is public, the way to authenticate and effectuate the transfer of these assets is to use public and private keys that are assigned to these assets.

46. Each cryptocurrency address has one public key and one private key assigned to 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.

47. The private key, however, is the sole mechanism that allows the transfer of cryptocurrency. With the private key, an individual can implement an untraceable transfer of the cryptocurrency from one computer to another. Conversely, without the private key, cryptocurrency cannot be transferred. Anyone with a cryptocurrency's private key, therefore, has total control over the

funds in a portfolio. This key comes in many forms and must be kept private to avoid having control over an individual's portfolio.

C. Cryptocurrency Security

48. As their name suggests, mathematically encoded cryptographic private keys are at the heart of cryptocurrency transactions. These keys are extremely secure in that they are nearly impossible to determine or generate without an owner's input.

49. Nonetheless, there have, however, been targeted attacks used to steal cryptocurrencies by luring users into disclosing their private keys. One of the largest Bitcoin exchanges, for example, lost a staggering $280 Million in Bitcoin as recently as 2021.[5]

50. Because it is nearly impossible to guess a ser's private access key, hackers employ targeted attacks aimed at luring users into disclosing their private keys. Once a hacker gains access to these keys, the hacker controls its funds and can transfer them with impunity. Unlike accounts that store currency electronically through banks or investment funds, there is no approval process for moving cryptocurrency assets. Any transfer are additionally untraceable and irreversible, leaving the recipient immune from identification or consequences for their actions.

51. Security over a user's private portfolio keys is therefore of the utmost importance.

D. Ledger Wallets

52. The need for security over private access keys is where Ledger hardware wallets enter the picture. Ledger Wallets allow customers to purchase a physical device that in turn uses an online application and other customer services for cryptocurrency owners to control and monitor their cryptocurrency portfolios.

[5] Ada Hui, Wolfie Zhao, *Over $280M Drained in KuCoin Crypto Exchange Hack*, COINDESK (Sept. 14, 2021), https://www.coindesk.com/markets/2020/09/26/over-280m-drained-in-kucoin-crypto-exchange-hack/.

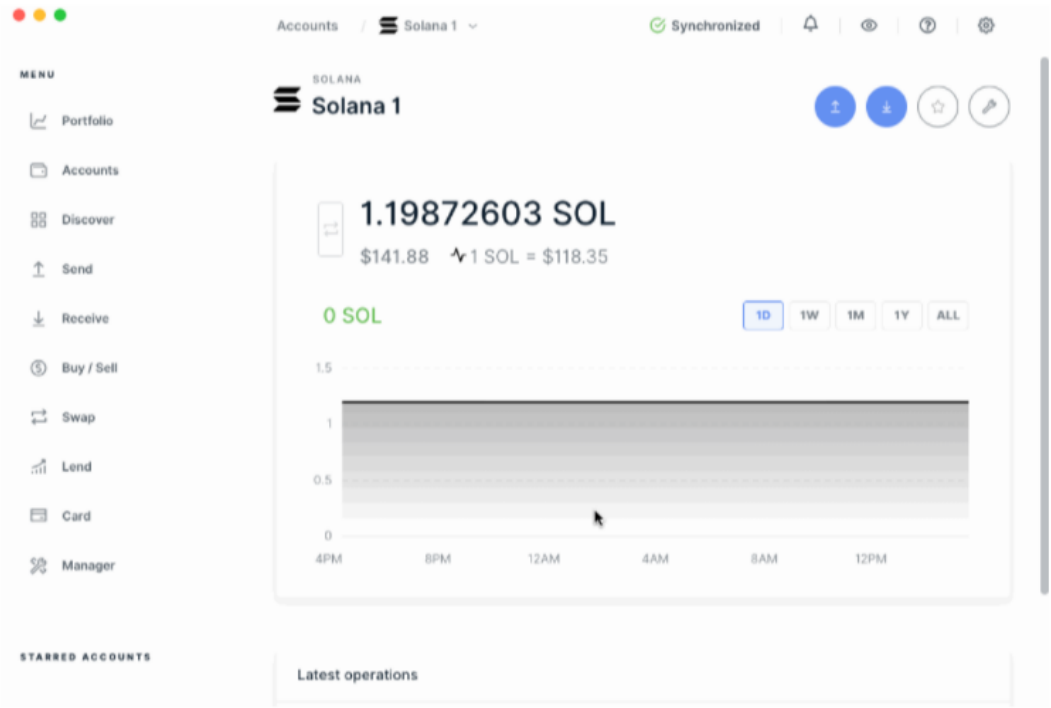
53. The "hardware wallets" that Ledger sells are physical products that look like portable USB hard drives. Below is an example of such a Ledger hardware wallet:

54. The point of these "wallets" is not to store cryptocurrency inside of them like a traditional wallet stores physical currency. Cryptocurrency investors, rather, use the hardware wallet to store their private keys in a physical device that is not held online, and thus is marketed as a safer way of storing a user's cryptocurrency portfolio keys.

55. The Ledger Wallet itself is secured with a PIN number or password, meaning that misplacing the wallet does not pose a risk of theft.

56. Ledger also maintains an online customer service application called "Ledger Live," which interacts with users' devices and allows Ledger Wallet owners to transfer, buy, sell, and receive various crypto-assets. Below is a screenshot of this functionality:

Solana support is only available as an experimental feature for now. To create a Sola account and manage SOL in Ledger Live, go to **Settings** > **Experimental features** a activate **Experimental integrations** by using the toggle button.



For more information on how to manage SOL in Ledger Live, refer to the following article: Solana (SOL).

57. Ledger, through the purchase of the wallet devices and the use of the Ledger Live services, collects and processes the PII of its consumers, including, but not limited to first and last names, email addresses, post addresses, and telephone numbers. *See also* ¶ 5, *supra.*

58. This PII was collected by Ledger when Plaintiffs and the Class purchased their Ledger hardware devices and signed up for the Ledger Live online services.

E. Hacking of Hardware Wallets

59. Users of hardware wallets generally face risks of theft of their private keys, usually targeted at where those keys are stored. If an owner stores their hardware keys on a personal computer or other electronic device, then that device may be the target of hacking

attempts aimed at gaining access to that device's internal drive containing the passkey information. Physical hardware wallets, however, are not connected to the internet, and hackers must therefore utilize targeted attempts to gain a user's passkey by luring them into revealing it, either online in a fake form response or directly to a cybercriminal. These attacks are usually in the form of phishing attacks, SIM-swap attacks, or physical intimidation, in which cybercriminals will force users into paying money or revealing their passcode to a hacker.

60. Phishing attacks entail a cybercriminal purporting to be a legitimate business or institution and contacting targets with the goal of luring them into revealing a passkey when they otherwise would not. Examples of phishing attacks include 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.

61. SIM-swap attacks occur when an attacker gains control of an individual's phone number by convincing the individual's mobile carrier to switch the number to a new SIM-card that the attacker possesses. The attacker can then gain control of that phone number and bypass authentication pages that force the user to verify their phone number.

62. Users of devices like the Ledger Wallet are, by the nature of their investments, more skeptical of these phishing attempts and are aware of cybercriminals' attempts to fraudulently procure cryptocurrency in recent years. Ledger users will commonly create unique email addresses used just for interacting with accounts that manage their crypto assets. Ledger users also have a separate dedicated phone number to use for dual-factor authentication when interacting with their cryptocurrencies. By implementing these additional security measures,

users know that cryptocurrency related emails to other email addresses and phone numbers are illegitimate.

63. Plaintiffs took some of these additional security measures in addition to buying a Ledger hardware wallet. Mr. Kissinger, for example, continuously updated his email password and implemented additional verification steps on the email address that he used to manage his cryptocurrency portfolios. Additionally, Plaintiff Sipprell used an entirely separate phone number and email account for the management of his cryptocurrency portfolio through his Ledger Nano device. By using a dedicated phone number and email address, Plaintiff Sipprell took the extra step of eliminating the risk of being lured into divulging his passkey information through phishing attacks on contact information that hackers could piece together from sources other than the Ledger data breach incident. Any communications related to his Ledger device or cryptocurrency portfolio on other emails would have immediately been recognized as spam by Plaintiff Sipprell, yet the hackers had access to his dedicated Ledger email and phone number, making these phishing attacks even more sophisticated and targeted towards specific Ledger users. This underscores the importance of securing this information.

64. For these reasons, the only point of vulnerability for owners of Ledger Wallets is public disclosure of the PII of the wallet's owner. If hackers know the names, email addresses, phone numbers, or physical addresses of people who own Ledger Wallets, ingenious phishing attempts can be engineered to target users' dedicated crypto-trading accounts. All that would need to be accomplished once this information was known is that the cybercriminals convince the user that they are receiving a communication from Ledger itself, leading to the disclosure of their secure passkeys and allowing the criminals to drain the users' cryptocurrency.

65. A great deal of information is also available about Plaintiffs and class members on the dark web. This information imposes further uncompensated costs on those individuals. The dark web allows cybercriminals to piece information about cryptocurrency investors together, revealing blockchain records that can allow other hackers to monitor a user's portfolio, including how much currency is in an account.

F. The Data Breach

66. Making unequivocal representations about the security of its devices noted above, despite knowing such representations were not true relating to its own data security practices and those of its data processing vendors, Shopify and TaskUs, Ledger sold Plaintiffs and Class members the Ledger Nano X and Ledger Nano S wallets for $119 and $59, respectively.

i. Ledger Uses Shopify as an e-Commerce Vendor

67. Ledger sells its Nano products through number of distributers, including Amazon and Walmart. It also sells the devices directly to customers through its own website.

68. Shopify powers Ledger's website. Shopify is a large e-commerce company. Over a million businesses use its platform, and over $64 Billion of sales occurred on its platform through these businesses in 2019. Shopify is the largest publicly-traded company in Canada.

69. 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.

70. When users purchase directly from Ledger on its Shopping Website or sign up for the Ledger Live services 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.

71. 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."

ii. Shopify Uses TaskUs as a Data-Processing Company for Ledger Data

72. TaskUs is a U.S. based outsourcing company that provides a number of internet-based content services to hundreds of companies, including customer technical support, content moderation, and data security.

73. Upon information and belief, TaskUs was contracted by Shopify to provide customer support and data security consulting services for Ledger's sales website and the Ledger Live services, in which Ledger customers could obtain live support for their investments and effectuate transfers of their assets on Ledger's website. Specifically, TaskUs was entrusted with the information collected by the Ledger Live service and the Ledger website, described above in ¶ 5, *supra*, via Shopify, Inc.'s collection of the data through Shopify, Inc.'s e-commerce services to Ledger. TaskUs therefore had access to and was entrusted with the sensitive user PII that would allow cybercriminals to target Ledger users with sophisticated phishing attacks.

74. TaskUs's privacy policy specifically mentions that it collects the types of PII that were leaked in the Data Breach through third parties that use the company's services.[6] The

[6] *See Privacy* Statement, TASKUS (July 28, 2021), https://www.taskus.com/privacy-statement/.

company notes in its privacy policy that it takes "reasonable measures to protect your Personal Information against loss, destruction, alteration, or unauthorised access or disclosure."

iii. The Data Breach

75. Between April and June of 2020, certain "rogue" TaskUs employees took advantage of the Ledger customer information provided to the company through Shopify's e-commerce services and acquired and exported Ledger's customer transactional records. The TaskUs employees also obtained data relating to other merchants.

76. On September 22, 2020, Shopify announced that "two rogue members of our support team were engaged in a scheme to obtain customer transactional records of certain merchants," involving "the data of less than 200 merchants" and that their support teams had "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 and TaskUs knew of the Data Breach more than a week before this announcement.

77. On February 19, 2021, a federal grand jury indicted a California hacker by the pseudonym "Pokeball" for wire fraud related to his role in causing the Data Breach.[7] The indictment alleges that starting in May 2019, Pokeball paid an employee of a Shopify vendor to provide him with Shopify's merchant data. Upon information and belief, TaskUs was the Shopify vendor involved in the Data Breach and acted as Shopify's agent, providing customer support services to Shopify customers on its behalf.

[7] *See* Criminal Indictment, *United States v. Heinrich*, 8:21-cr-22-JLS (C.D. Cal. 2021), Docket No. 16 at 2.

78. The Data Breach involved the data of approximately 272,000 people, approximately a third of whom live in the United States. Hackers copied information such as names, order details, email addresses, physical addresses, and phone numbers. And for many other users, hackers obtained the email address users registered when buying their Ledger Wallets.

79. By the time it publicly announced the Data Breach, Shopify notified every affected merchant that rogue employees had stolen their data, but neither Shopify nor TaskUs warned the hundreds of thousands of individuals harmed by the Data Breach. Instead, TaskUs and Shopify attempted to cover up and downplay the scale of the Data Breach and did nothing to protect the owners of data Shopify and TaskUs had been entrusted with.

iv. Ledger Initially Denies the Extent of the Data Breach

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

81. This publicly-stated concern was an opportunity for Shopify and Taskus to get ahead of the problem. Shopify and TaskUs should have, at a minimum: (1) disclosed the Data 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.

82. During this time, the risks and damages to Ledger's customers were only increasing. A prompt and proper response from Shopify and TaskUs, including full disclosure to

[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-custome

all vendors and customers involved in the Data Breach, would have mitigated those risks and damages.

v. The Data Breach is Acknowledged Publicly for the First Time

83. On July 29, 2020, Ledger partially admitted that it was involved in the Data Breach, yet neither TaskUs nor Shopify had made any attempts to notify affected Ledger customers of the incident.

84. 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 of 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.**
>
> **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.**

85. This disclosure effort was flawed and misleading. Namely, Shopify and TaskUs did not immediately warn affected customer and instead took months to "investigate" the claims against their data storage practices. Shopify and TaskUs did even not disclose the Data Breach to any customers, let alone explain the extent of the Data Breach, where the information was lost, and who it may have been lost to.

86. Ledger customers were still completely in the dark about the extent of the loss of this information at this point. All they had received by way of communication from Shopify and TaskUs was an update from Ledger that it was "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 Data 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.

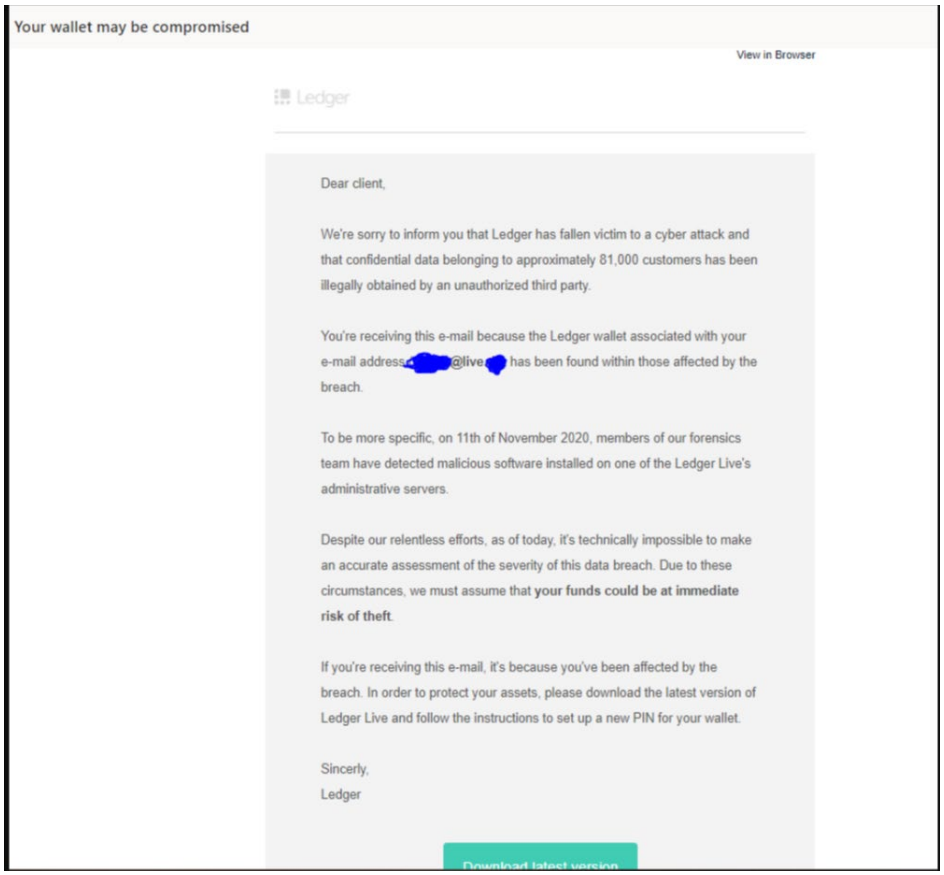
vi. Attacks on Ledger Users Increase Exponentially

87. By fall of 2020, Ledger, Shopify, and TaskUs did not even attempt to respond to reports that Ledger customers had faced severe threats or had seen millions of dollars in

cryptocurrency untraceably removed from their accounts. Shopify had not disclosed to its customers that it had any connection with the Data Breach. It had not contacted every customer who had their information lost in the Data Breach, nor had it provided sufficient disclosures to assist customers whose information may have been lost. TaskUs, by this point, had not even disclosed that it was the third-party contractor who had been processing this Shopify e-commerce data, and sat back while media reports of phishing attacks and the loss of cryptocurrency through the Ledger breach increased.

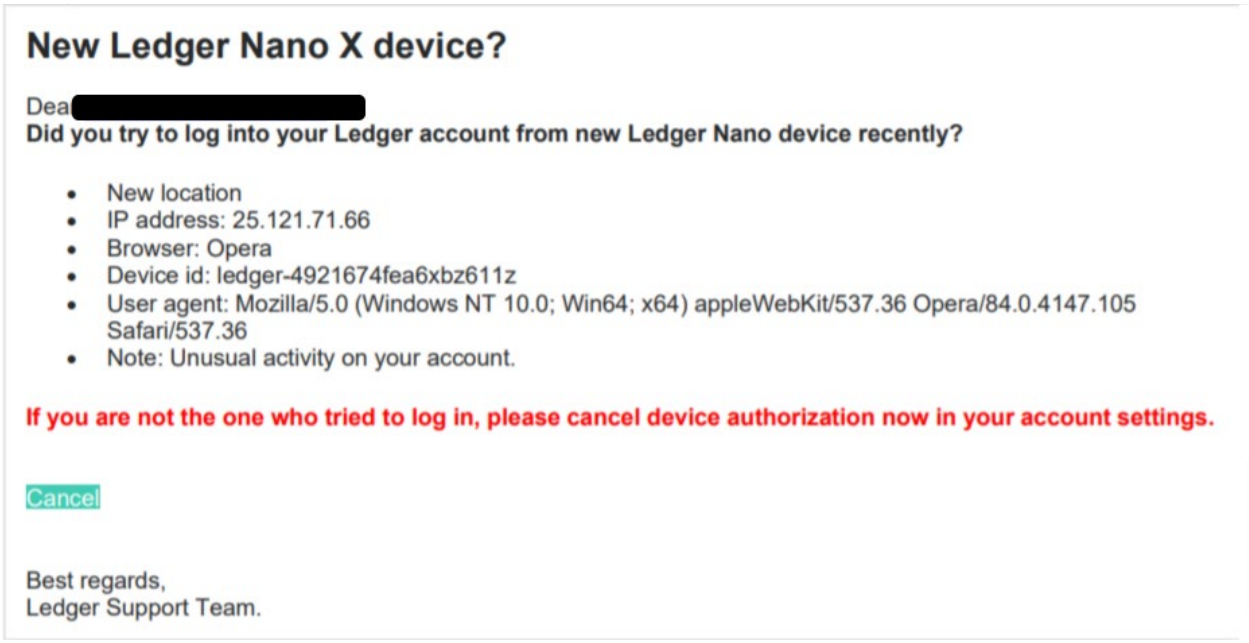
88. Meanwhile, as Shopify and TaskUs continued to leave customers in the dark about the extent of the Data Breach, Plaintiffs and Class members began receiving high volumes of phishing emails, SIM-swap attacks, and intimidation threats, with no warning about where these attacks may be coming from, or how to avoid them. These emails looked like emails sent from Ledger support.

89. In November 2020, for example, a Ledger user reported a phishing attempt by hackers posing as the Ledger support team members and asking Ledger customers to download fake version of the Ledger Live software. The fake email was extremely convincing and was sent to the email addresses that Ledger users had registered their devices on:



90. Other Ledger users responded to the report by confirming that they had received and been tricked by the fake emails. One user reported: "Got 2 of them in 20 minutes this afternoon. The only thing they have is our e-mail address. They want us to install the so-called "latest version of Ledger Live" with a link in the mail, which is a typical red light. I wonder how many of the non tech-saavy Ledger owners who will fall in this trap…"

91. Plaintiffs received these phishing emails from the hackers pretending to be Ledger support staff. Plaintiff Sipprell, for example, received a phishing email in December of 2020 that appeared to be from Ledger:



New Ledger Nano X device?

Dea[redacted]

Did you try to log into your Ledger account from new Ledger Nano device recently?

- New location
- IP address: 25.121.71.66
- Browser: Opera
- Device id: ledger-4921674fea6xbz611z
- User agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) appleWebKit/537.36 Opera/84.0.4147.105 Safari/537.36
- Note: Unusual activity on your account.

If you are not the one who tried to log in, please cancel device authorization now in your account settings.

Cancel

Best regards,
Ledger Support Team.

92. The hackers behind this fake email were of course armed with Ledger's customer lists and email addresses, and were therefore aware that they were targeting Ledger customers. These hackers invested time and resources to create convincing fake emails that were successful. Worst yet, because of Ledger, Shopify, and TaskUs's failure to admit to the scope of the Data Breach at this point in the timeline, many of Ledger's customers did not know that they emails had been compromised.

93. The hacking attempts were not limited to emails. Ledger users reported the receipt of SMS/text phishing attempts from actors claiming to be Ledger, as well as SIM-swap attacks. These attacks occurred when scammers trick a wireless telephone carrier into porting the victim's phone number to the criminal's SIM card. By doing so, the attacker is able to bypass two-factor authentication security on websites, including the Ledger Live service.

94. But for Defendants' unlawful conduct, hackers would not have accessed Plaintiffs' and the putative class members' contact information. Defendants' unlawful conduct—including active attempts to conceal the Data Breach and minimize the extent of the Data Breach or damages—has directly and proximately resulted in widespread digital attacks against Plaintiffs and the putative class.

95. In addition to these types of threats, Plaintiffs and Class members' home addresses are now public online. The class as a whole is comprised of a group of people who are at an especially high risk of ransom threats and blackmail attempts. But for Defendants' unlawful conduct, such criminals would not have access to the home or other postal addresses of Plaintiffs and the Class. This access has result in, at minimum, an invasion of Plaintiffs' and the Class's privacy and can lead to even greater damages, including theft or violent physical attacks.

vii. Severe Emotional Distress and Fear experienced by Ledger users

96. The actions described herein have resulted in severe emotional distress for Plaintiffs and the Class. Plaintiffs and the Class have lost all security and privacy over important financial information, as well as their home addresses, names, and other contact information in addition to the fact that they lost millions of dollars from the targeted attacks in the Data Breach.

97. Plaintiff Kissinger, for example, had to seek help from a mental health professional to cope with the ensuing panic attack that resulted from the loss of his cryptocurrency from his Ledger account, with his emotions continually on edge about the incident.

98. Plaintiffs and the Class remain on edge and alert as they are bombarded with phishing emails and other scams. Plaintiffs are suffering from the metal and emotional distress associated with such insecurity and uncertainty caused by the Data Breach. Plaintiff Kissinger

went into a state of depression after the Data Breach when the actual theft of his assets happened, and his personal and professional relationships have suffered. Class members, in addition to the huge financial loss and mental anguish they have been exposed to during the Data Breach, continue to suffer from stress, anxiety, depression, and financial problems as a result.

99. As long as Plaintiffs and the Class members' PII is accessible on the internet, Plaintiffs and the Class will remain at substantial risk. Shopify and TaskUs have not offered any solutions to remedy the damages to Plaintiffs and the Class. Plaintiffs and Class members remain at permanent risk unless they take on the significant time and expense to change all of the personal information that was exposed, including their home addresses.

viii. Ledger Finally Admits to the Scale of the Data Breach

100. In December 2020, reports continued to come in about phishing attempts on Ledger users. By that time, Ledger, TaskUs, and Shopify'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 references breaches and then instructed users, as a security measure, to install fake versions of Ledger Live that asked for their PII, or made near-exact copies of the Ledger device sign-in page that made users believe that another Ledger device had been linked to their email, luring them into frantically clicking on a fake "cancel" button that took them to a fake customer support website.

101. Plaintiffs, along with other Class members have reported losing significant sums of crypto-assets as a result of such phishing attempts. Plaintiff Forsberg believed that he was interacting with the Ledger customer support interface in December of 2020, which he received a link to through one of these phishing emails, resulting in the loss of approximately 6,000 XRP coins, worth anywhere from $3000-$5000 in today's money. Plaintiff Gunter fell victim to a

SIM-card swap in which approximately 3.99 Ethereum and .042 Bitcoin were transferred out of his account, resulting in approximately $11,130 worth of loss in today's money. Plaintiff Kissinger was similarly directed to a fake Ledger support website through a phishing text message that he received in November of 2020 in which hackers told him that someone had registered a Ledger device in his name without authorization, resulting in him inputting his credentials on the fake website and allowing the hackers to remove approximately $23,220 in cryptocurrency from his Ledger account. Finally, Plaintiff Sipprell was the victim of a phishing attack by email that resulted in the loss of approximately $100,000 worth of Stellar Lumens Coins from his Ledger Wallet. At the time of the phishing attack, Plaintiff Sipprell was in Florida.

102. The phishing attempts were sufficiently successful so that as the depth and scope of the Data Breach grew, hackers were paying up to $100,000.00 for the compromised list of ledger customer data.[9]

103. 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. In fact, the contents of the Ledger database entrusted to Shopify and TaskUs were distributed on Raidforums. Raidforums is a database sharing and marketing forum that distributes leaked information online. This leak of 272,000 pieces of detailed PII of consumers is significantly greater than he amount of data estimated by Ledger – of 9,500, an estimate reported by Ledger in July 2020.

[9] @UnderTheBreach, TWITTER (Dec. 20, 2020, 01:38 PM), https://twitter.com/UnderTheBreach/status/1340735356375851009.

104. Consumers and the media justly criticized Ledger and Shopify, stating that the companies had "vastly underestimated" the Data Breach.[10]

105. With the data made publicly available for free, many edger customers started receiving frightening threats. Ledger customers immediately started receiving spam phone calls, emails, and even death threats.

106. Plaintiffs Forsberg, Gunter, Kissinger, and Sipprell, like many members of the Class, also received numerous spam calls, emails, texts, and other communications attempting to phish for personal information and extort them out of their cryptocurrency assets. Plaintiffs' PII is now available for other parties to sell and trade, and they continue to risk receiving more harm for the indefinite future. Plaintiffs have also spent enormous amounts of time, usually measured in days, attempting to move their cryptocurrency out of their accounts and into more secure locations, changing cell phone numbers and bank accounts, as well as reporting the incidents to the FBI to attempt to find the missing cryptocurrency—all to no avail.

107. Importantly, the Data Breach exposed the physical addresses of the customers who lost their information in the Data Breach, meaning that users' home addresses will not be safe unless they move away from them.

108. Before the Data Breach, Shopify and TaskUs should have regularly deleted or archived customer data or should have otherwise protected that information from online accessibility. After the Data Breach, for more than five months, Shopify and TaskUs repeatedly failed to provide critical information to those affected by the Data Breach, compounding the damages suffered by Plaintiffs and Class members.

[10] *See Ledger Breach Vastly Underestimated, 270,000 Clients Data Leaked*, CRYPTOBRIEFING (Dec. 21, 2020), https://cryptonews.net/en/news/security/439897/.

109. TaskUs in particular failed to protect Ledger's customer data as well. TaskUs employees should not have had access to Ledger customer information, and the company should have limited employee access to customer data in a way that prevented rogue employees' access, monitored employees' computer use and copying of files from company servers, assisted Shopify with its investigation of the Data Breach, and notified Ledger customers of the loss of their information.

G. Damages to Plaintiffs and the Class

110. Plaintiffs Forsberg, Gunter, Kissinger, and Sipprell have suffered damages from the Data Breach as set forth above.

111. If Shopify and TaskUs had disclosed the extent of the Data Breach—instead of waiting for over six months—some Plaintiffs, sophisticated users with technology backgrounds and wary of scams, would have been on heightened alert and not fallen prey to these scams. Furthermore, others who may not have been of a sophisticated technology background could have taken additional steps to protect their privacy rights.

112. As to other forms of damages, Plaintiffs' emails and personal information have been compromised. Plaintiffs Forsberg, Gunter, and Sipprell have received a huge amount of phishing and other scam emails and text messages.

113. The Data Breach has also exposed the locations of purchased Ledger products, by allowing access to Plaintiffs' and other customers' home addresses, which inherently impacts the security of products like the Ledger Wallet that use home addresses to keep login information secure.

114. Some Class members also remain fearful that intruders will harm them in their homes due to their addresses being leaked publicly.

115. These leaks of personal information, in conjunction with the information that they were Ledger customers, has exposed Plaintiffs to additional risks of theft and fraud.,

116. Had Plaintiffs been made aware of Defendants' lax data security practices, unwillingness to promptly and completely disclose data breaches such as this one, and failure to provide timely customer service, Plaintiffs would not have provided any PII to Ledger or stored any bitcoins or other forms of cryptocurrency in their Ledger Wallets; nor would Plaintiffs have agreed to allow their information to be transmitted to Shopify or TaskUs.

V. CLASS ALLEGATIONS

117. Plaintiffs bring this Action as a class action pursuant to Fed. R. Civ. P. 23 and seek certification of the following Nationwide Class and State Subclasses (collectively defined as the "Class"):

> Nationwide Class: All persons residing in the United States who provided Shopify or TaskUs with personal information (through the use of a Ledger Wallet) that was accessed, compromised, stolen, or exposed in the Data Breach.
>
> Arizona Subclass: All persons residing in Arizona who provided Shopify or TaskUs with personal information (through the use of a Ledger Wallet) that was accessed, compromised, stolen, or exposed in the Data Breach.
>
> Florida Subclass: All persons residing in Florida who provided Shopify or TaskUs with personal information (through the use of a Ledger Wallet) that was accessed, compromised, stolen, or exposed in the Data Breach.
>
> Kentucky Subclass: All persons residing in Kentucky who provided Shopify or TaskUs with personal information (through the use of a Ledger Wallet) that was accessed, compromised, stolen, or exposed in the Data Breach.
>
> North Carolina Subclass: All persons residing in North Carolina who provided Shopify or TaskUs with personal information (through the use of a Ledger Wallet) that was accessed, compromised, stolen, or exposed in the Data Breach.

The Class Period shall be April 1, 2020 through the present.

118. Excluded from the Class 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.

119. Certification of Plaintiffs' claims for class-wide treatment is appropriate because Plaintiffs can prove the elements of the claims on a class-wide basis using the same evidence as would be used to prove those elements in individual actions alleging the same claims.

120. Numerosity—Federal Rule of Civil Procedure 23(a)(1). The members of the Class are so numerous that joinder of all Class members would be impracticable. On information and belief, the Class numbers in the thousands. Moreover, the Class and Subclasses are composed of an easily ascertainable set of individuals who had Ledger Wallets and were thus impacted by the Data Breach. The precise number of Class members has already been ascertained and can be further confirmed through discovery, which includes Defendants' records. The disposition of Plaintiffs and Class members' claims through a class action will benefit the parties and this Court.

121. **Commonality and Predominance—Federal Rule of Civil Procedure 23(a)(2) and 23(b)(3).** Common questions of law and fact exist as to all members of the Class and predominate over questions affecting only individual members of the Class. Such common questions of law or fact include, *inter alia*:

- Whether Defendants' data security systems and/or protocol prior to and during the Data Breach complied with applicable data security laws and regulations;
- Whether Defendants' data security systems and/or protocol prior to and during the Data Breach were consistent with industry standards;
- Whether Defendants properly implemented their purported security measures to

protect Plaintiffs' and the Class's PII from unauthorized capture, dissemination, and misuse;

- Whether Defendants took reasonable measures to determine the extent of the Data Breach after it first learned of same;

- Whether Defendants disclosed Plaintiffs' and the Class's PII in violation of the understanding that the PII was being disclosed in confidence and should be maintained;

- Whether Defendants willfully, recklessly, or negligently failed to maintain and execute reasonable procedures designed to prevent unauthorized access to Plaintiffs' and the Class's PII;

- Whether Defendants were negligent in failing to properly secure and protect Plaintiffs' and the Class's PII;

- Whether Defendants were unjustly enriched by their actions; and

- Whether Plaintiffs and the other members of the Class are entitled to damages, injunctive relief, or other equitable relief, and the measure of such damages and relief.

122. Defendants engaged in a common course of conduct giving rise to the legal rights sought to be enforced by Plaintiffs, on behalf of themselves and other members of the Class. Similar or identical common law violations, business practices, and injuries are involved. Individual questions, if any, pale by comparison, in both quality and quantity, to the numerous common questions that predominate in this action.

123. **Typicality—Federal Rule of Civil Procedure 23(a)(3).** Plaintiffs' claims are typical of the claims of the other members of the Class because, among other things, all Class members were similarly injured and sustained similar monetary and economic injuries as a result of Defendants' uniform misconduct described above and were thus all subject to the Data Breach alleged herein. Further, there are no defenses available to Defendants that are unique to Plaintiffs.

124. **Adequacy of Representation—Federal Rule of Civil Procedure 23(a)(4).** Plaintiffs are adequate representatives of the Class because their interests do not conflict with the interests of the Class they seek to represent, they have retained counsel competent and experienced in complex class action litigation, and Plaintiffs will prosecute this action vigorously. The Class's interests will be fairly and adequately protected by Plaintiffs and their counsel.

125. **Injunctive Relief—Federal Rule of Civil Procedure 23(b)(2).** Defendants have acted and/or refused to act on grounds that apply generally to the Class, making injunctive and/or declaratory relief appropriate with respect to the Class under Fed. Civ. P. 23 (b)(2).

126. **Superiority—Federal Rule of Civil Procedure 23(b)(3).** A class action is superior to any other available means for the fair and efficient adjudication of this controversy, and no unusual difficulties are likely to be encountered in the management of this class action. The damages or other financial detriment suffered by Plaintiffs and the other members of the Class are relatively small compared to the burden and expense that would be required to individually litigate their claims against Defendants, so it would be impracticable for members of the Class to individually seek redress for Defendants' wrongful conduct. Even if members of the Class could afford individual litigation, the court system could not. Individualized litigation creates a potential for inconsistent or contradictory judgments and increases the delay and expense to all parties and the court system. By contrast, the class action device presents far fewer management difficulties and provides the benefits of a single adjudication, economy of scale, and comprehensive supervision by a single court.

127. Class certification is also appropriate under Rules 23(b)(1) and/or (b)(2) because:

- The prosecution of separate actions by the individual members of the Class would create a risk of inconsistent or varying adjudications establishing incompatible

standards of conduct for Defendants;

- The prosecution of separate actions by individual Class members would create a risk of adjudication that would, as a practical matter, be dispositive of the interests of other Class members not parties to the adjudications, or would substantially impair or impede their ability to protect their interests; and

- Defendants have acted and refused to act on grounds generally applicable to the Class, thereby making appropriate final injunctive relief with respect to the members of the Class as a whole.

128. Class certification is also appropriate because this Court can designate particular claims or issues for class-wide treatment and may designate multiple subclasses pursuant to Fed. R. Civ. P. 23(c)(4).

129. No unusual difficulties are likely to be encountered in the management of this action as a class action.

COUNT I
NEGLIGENCE
(On Behalf of Plaintiffs and the Nationwide Class or, alternatively, the State Subclasses)

130. Plaintiffs incorporate the preceding paragraphs as though fully set forth herein.

131. Upon Defendants' accepting and storing the PII of Plaintiffs and the Class in its computer systems and on its networks, Defendants undertook and owed a duty to Plaintiffs and the Class to exercise reasonable care to secure and safeguard that information and to use commercially reasonable methods to do so. Defendants knew that the PII was private and confidential and should be protected as private and confidential.

132. Defendants owed a duty of care not to subject Plaintiffs' and the Class's PII to an unreasonable risk of exposure and theft because Plaintiffs and the Class were foreseeable and probable victims of any inadequate security practices.

133. Defendants owed numerous duties to Plaintiffs and the Class, including the following:

- to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting and protecting PII in its possession;
- to protect PII using reasonable and adequate security procedures and systems that are compliant with industry-standard practices; and
- to implement processes to quickly detect a data breach and to timely act on warnings about data breaches.

134. Defendants also breached their duty to Plaintiffs and Class members to adequately protect and safeguard PII by disregarding standard information security principles, despite obvious risks, and by allowing unmonitored and unrestricted access to unsecured PII. Furthering their dilatory practices, Defendants failed to provide adequate supervision and oversight of the PII with which it was and is entrusted, in spite of the known risk and foreseeable likelihood of breach and misuse, which permitted a malicious third party to gather Plaintiffs' and Class members' PII and potentially misuse the PII and intentionally disclose it to others without consent.

135. Defendants knew, or should have known, of the risks inherent in collecting and storing PII and the importance of adequate security.

136. Defendants knew, or should have known, that their data systems and networks did not adequately safeguard Plaintiffs' and Class members' PII.

137. Defendants breached their duties to Plaintiffs and Class members by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiffs' and Class members' PII.

138. Because Defendants knew that a breach of its systems would damage thousands of its customers, including Plaintiffs and Class members, Defendants had a duty to adequately protect their data systems and the PII contained thereon.

139. Defendants' duty of care to use reasonable security measures arose as a result of the special relationship that existed between Defendants and its customers, which is recognized by laws and regulations including but not limited to common law. Defendants were in a position to ensure that its systems were sufficient to protect against the foreseeable risk of harm to Class members from a data breach.

140. In addition, Defendants had a duty to employ reasonable security measures under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data.

141. Defendants' duty to use reasonable care in protecting confidential data arose not only as a result of the statutes and regulations described above, but also because Defendants were bound by industry standards to protect confidential PII.

142. Defendants' own conduct also created a foreseeable risk of harm to Plaintiffs and Class members and their PII. Defendants' misconduct included failing to: (1) secure Plaintiffs' and Class member's PII; (2) comply with industry standard security practices; (3) implement adequate system and event monitoring; and (4) implement the systems, policies, and procedures necessary to prevent this type of data breach.

143. Defendants breached their duties, and thus were negligent, by failing to use reasonable measures to protect Class members' PII, and by failing to provide timely notice of the Data Breach. The specific negligent acts and omissions committed by Defendants include, but

are not limited to, the following:

- Failing to adopt, implement, and maintain adequate security measures to safeguard Class members' PII;
- Failing to adequately monitor the security of Defendants' networks and systems;
- Allowing unauthorized access to Class members' PII;
- Failing to detect in a timely manner that Class members' PII had been compromised; and
- Failing to timely notify Class members about the Data Breach so that they could take appropriate steps to mitigate the potential for identity theft and other damages

144. Through Defendants' acts and omissions described in this Complaint, including their failure to provide adequate security and failure to protect Plaintiffs' and Class members' PII from being foreseeably captured, accessed, disseminated, stolen and misused, Defendants unlawfully breached their duty to use reasonable care to adequately protect and secure Plaintiffs' and Class members' PII during the time it was within Defendants' possession or control.

145. Defendants' conduct was grossly negligent and departed from all reasonable standards of care, including, but not limited to failing to adequately protect the PII and failing to provide Plaintiffs and Class members with timely notice that their sensitive PII had been compromised.

146. Neither Plaintiffs nor the other Class members contributed to the Data Breach and subsequent misuse of their PII as described in this Complaint.

147. As a direct and proximate result of Defendants' conduct, Plaintiffs and Class members suffered damages as alleged above.

148. Plaintiffs and Class members are also entitled to injunctive relief requiring Defendants to, *e.g.*, (i) strengthen data security systems and monitoring procedures; and (ii) submit to future annual audits of those systems and monitoring procedures.

COUNT II
NEGLIGENCE PER SE
(On Behalf of Plaintiffs and the Nationwide Class or, alternatively, the State Subclasses)

149. Plaintiffs fully incorporate by the proceeding paragraphs as though fully set forth herein.

150. 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 Defendants' duties.

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

152. Shopify and TaskUs's violations of Section 5 of the FTC Act (and similar state consumer protection statutes) constitute negligence per se. This negligence was, at the very minimum, a substantial factor in causing the Plaintiffs' and Class members' PII to be improperly accessed, disclosed, and otherwise compromised, and in causing Plaintiffs' and Class members' other injuries as a result of the Data Breach.

153. 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.

154. As a direct and proximate result of Shopify's and TaskUs'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.

COUNT III
DECLARATORY JUDGMENT AND INJUNCTIVE RELIEF
(On Behalf of Plaintiffs and the Nationwide Class or, alternatively, the State Subclasses)

155. Plaintiffs fully incorporate by reference all of the above paragraphs, as though fully set forth herein.

156. 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.

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

158. Plaintiffs allege that Defendants' data-security measures remain inadequate. Shopify and TaskUs deny these allegations. In addition, Plaintiffs continue to suffer injury as a result of the compromise of their PII and remain at imminent risk that further compromises of their PII and continued fraudulent activity against them will occur in the future.

159. Pursuant to its authority under the Declaratory Judgment Act, Plaintiffs ask the Court to enter a judgment declaring, among other things, the following: (i) Shopify and TaskUs owe a duty to secure consumers' PII and to timely notify consumers of a data breach under the common law, Section 5 of the FTC Act, and various state statutes; and (ii) Shopify and TaskUs are in breach of these legal duties by failing to employ reasonable measures to secure consumers' PII in their possession and control.

160. Plaintiffs further ask the Court to issue corresponding prospective injunctive relief requiring Shopify and TaskUs to employ adequate security protocols consistent with law and industry standards to protect consumers' PII from future data breaches.

161. 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 Shopify and/or TaskUs. The risk of another such breach is real, immediate, and substantial. If another breach at TaskUs 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 Class members will be forced to bring multiple lawsuits to rectify the same misconduct.

162. The hardship to the Class members if an injunction does not issue exceeds the hardship to Shopify and TaskUs if an injunction is issued. Among other things, if another massive data breach occurs due to the misconduct of Shopify and TaskUs, the Class members will likely be subjected to substantial hacking attempts, physical threats, and other damage, in

addition to the hacking attempts, physical threats, and damages already suffered. On the other hand, the cost to Shopify and TaskUs of complying with an injunction by employing reasonable prospective data security measures is relatively minimal, and Shopify and TaskUs have pre-existing legal obligations to employ such measures.

163. 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 Shopify and/or TaskUs, 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.

COUNT IV
UNJUST ENRICHMENT
(On Behalf of Plaintiffs and the Nationwide Class or, alternatively, the State Subclasses)

164. Plaintiffs fully incorporate by reference all of the above paragraphs, as though fully set forth herein.

165. Plaintiffs and Class members conferred a monetary benefit on Defendants. Specifically, they purchased goods and services from Defendants and provided Defendants with their Private Information. In exchange, Plaintiffs and Class members should have received from Defendants the goods and services that were the subject of the transaction and should have been entitled to have Defendants protect their Private Information with adequate data security.

166. Defendants knew that Plaintiffs and Class members conferred a benefit upon them and has accepted or retained that benefit. Defendants profited from Plaintiffs' purchases and used Plaintiffs' and Class members' Private Information for business purposes.

167. Defendants failed to secure Plaintiffs' and Class members' Private Information and, therefore, did not provide full compensation for the benefit the Plaintiffs' and Class members'

Private Information provided.

168. Defendants acquired the Private Information through inequitable means as they failed to disclose the inadequate security practices previously alleged.

169. If Plaintiffs and Class members knew that Defendants would not secure their Private Information using adequate security, they would have made alternative choices that excluded Defendants.

170. Plaintiffs and Class members have no adequate remedy at law.

171. Under the circumstances, it would be unjust for Defendants to be permitted to retain any of the benefits that Plaintiffs and Class members conferred on them.

172. Defendants should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiffs and Class members, proceeds that they unjustly received from them. In the alternative, Defendants should be compelled to refund the amounts that Plaintiffs and Class members overpaid.

COUNT V
Violation of Florida's Deceptive and Unfair Trade Practices Act ("FDUTPA")
Fla. Stat. § 501.201, *et seq.*
(On Behalf of Plaintiffs and the Nationwide Class or, alternatively, the Florida Subclass)

173. Plaintiffs fully incorporate by reference all of the above paragraphs, as though fully set forth herein.

174. Plaintiffs, Plaintiffs, class members, and Defendants each qualify as a person engaged in trade or commerce as contemplated by the Florida Deceptive and Unfair Trade Practices Act ("FDUTPA") Fla. Stat. § 501.201, *et seq.*

175. As alleged herein in this Complaint, Defendants engaged in unfair or deceptive acts or practices in the conduct of consumer transactions in violation of the FDUTPA, including but not limited to:

a. representing that its services were of a particular standard or quality that it knew or should have known were of another;

b. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiffs and class members' Private Information, which was a direct and proximate cause of the Data Breach;

c. Failing to identify foreseeable security and privacy risks, and remediate identified security and privacy risks, which was a direct and proximate cause of the Data Breach;

d. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs and class members' Private Information, including duties imposed by the FTCA, 15 U.S.C. § 45, which was a direct and proximate cause of the Cyber-Attack and data breach;

e. Misrepresenting that it would protect the privacy and confidentiality of Plaintiffs' and class members' Private Information, including by implementing and maintaining reasonable security measures;

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiffs' and Class members' Private Information; and

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and class members' Personal Information, including duties imposed by the FTCA, 15 U.S.C. § 45, which was a direct and proximate cause of the Security breach.

176. Defendants' representations and omissions were material because it was likely to deceive reasonable consumers about the adequacy of Defendant's data security and ability to protect the confidentiality of consumers' Private Information.

177. In addition, Defendant's failure to secure consumers' PHI violated the FTCA and therefore violates the FDUTPA.

178. Defendants knew or should have known that their computer systems and data security practices were inadequate to safeguard the PII of Plaintiffs and Class Members, deter hackers, and detect a breach within a reasonable time, and that the risk of a data breach was highly likely.

179. The aforesaid conduct constitutes a violation of the FDUTPA, Fla. Stat. § 501.204, in that it is a restraint on trade or commerce.

180. The Defendants' violations of the FDUTPA have an impact of great and general importance on the public, including Floridians. On information and belief, thousands of Floridians have used Defendants' services through their use of Ledger Wallets, many of whom have been impacted by the Data Breach. In addition, Florida residents have a strong interest in regulating the conduct of corporations who do business in Florida such as Defendants, whose policies and practices described herein affected millions across the country.

181. As a direct and proximate result of Defendants' violation of the FDUTPA, Plaintiffs and class members are entitled to a judgment under Fla. Stat. § 501.201, *et seq*, to enjoin further violations, to recover actual damages, to recover the costs of this action (including reasonable attorney's fees), and such other further relief as the Court deems just and proper.

182. Defendants' implied and express representations that they would adequately safeguard Plaintiff's and other class members' Private Information constitute representations as

to characteristics, uses or benefits of services that such services did not actually have, in violation of Fla. Stat. § 501.202(2).

183. Defendants' implied and express representations that they would adequately safeguard Plaintiff's and class members' Private Information constitute representations as to the particular standard, quality, or grade of services that such services did not actually have (as the data security services were of another, inferior quality), in violation of Fla. Stat. § 501.204.

184. Defendants knowingly made false or misleading statements in its privacy policy regarding the use of personal information submitted by members of the public in that Defendants advertised it is committed to protecting privacy and securely maintaining personal information. Defendant did not securely maintain personal information as represented, in violation of Fla. Stat. § 501.171.

185. These violations have caused financial injury to Plaintiffs and class members and have created an unreasonable, imminent risk of future injury.

186. Accordingly, Plaintiffs, on behalf of themselves and class members, bring this action under the Deceptive and Unfair Trade Practices Act to seek such injunctive relief necessary to enjoin further violations and to recover costs of this action, including reasonable attorneys' fees and costs.

COUNT VI
Violation of the North Carolina Unfair and Deceptive Trade Practices Act
N.C. Gen. Stat. § 75-1.1, *et seq*.
(On Behalf of Plaintiffs and the Nationwide Class or, alternatively, the North Carolina Subclass)

187. Plaintiffs fully incorporate by reference all of the above paragraphs, as though fully set forth herein.

188. The North Carolina Unfair and Deceptive Trade Practices Act, , N.C. Gen. Stat. § 75.1.1 ("UDTPA") "declare[s] unlawful" all "[u]nfair methods of competition in or affecting commerce, and unfair or deceptive acts or practices in or affecting commerce." *Id.* at § 75-1.1(a).

189. For the purposes of North Carolina's UDTPA, the term "commerce" includes all business activities, however, denominated, but does not include professional services rendered by a member of a learned profession.

190. Defendants violated the North Carolina UDTPA by engaging in unlawful, unfair, or deceptive business acts and practices in or affecting commerce, as well as unfair, deceptive, untrue, or misleading advertising that constitute acts of "unfair competition" prohibited in the statute.

191. Defendants engaged in unlawful acts and practices with respect to their services by establishing inadequate security practices and procedures described herein; by soliciting and collecting Plaintiffs' and Class Members' sensitive information with knowledge that such information would not be adequately protected; and by gathering Plaintiffs' and Class Members' sensitive information in an unsecure electronic environment in violation of North Carolina's data breach statute, the Identity Theft Protection Act, N.C. Gen. Stat. § 75-60, *et seq.*, which requires Defendants to undertake reasonable methods of safeguarding the sensitive information of the Plaintiffs and other Class Members.

192. In addition, Defendants engaged in unlawful acts and practices when they failed to discover and then disclose the data security breach to Plaintiffs and the Class Members in a timely and accurate manner, contrary to the duties imposed by N.C. Gen. Stat. § 75-65.

193. Defendants further violated UDTPA by violating North Carolina's Identity Theft Protection Act (ITPA), N.C. Gen. Stat. § 75-60, *et. seq.* ("ITPA") by: (a) Failing to prevent the PII

of Plaintiffs and Class Members from falling into unauthorized hands; (b) Failing to make reasonable efforts to safeguard and protect the PII of Plaintiffs and Class Members; (c) Failing to provide adequate notice of the security breach to affected consumers upon discovery that their system had been compromised and PII had been disclosed; and (d) In other ways to be discovered and proven at trial.

194. Defendants willfully concealed, suppressed, omitted and failed to inform Plaintiffs and Class Members of the material facts as described above.

195. As a direct and proximate result of Defendants' unlawful acts and practices, Plaintiffs and Class Members have been injured, suffering ascertainable losses and lost money or property, including but not limited to the loss of their legally protected interests in the confidentiality and privacy of their sensitive information.

196. Defendants knew or should have known that their data security practices were inadequate to safeguard Plaintiffs and the Class Members' sensitive information, that the risk of a data security breach was significant, and that their systems were, in fact, breached.

197. Defendants' actions in engaging in the above-named unlawful practices were negligent, knowing and willful, and/or wanton and reckless with respect to the rights of Plaintiffs and the Class Members.

198. Plaintiffs and the Class Members seek relief under the North Carolina UDTPA including, but not limited to: restitution to Plaintiffs and Class Members of money and property that Defendants have acquired by means of unlawful and unfair business practices; disgorgement of all profits accruing to Defendants because of their unlawful and unfair business practices; treble damages (pursuant to N.C. Gen. Stat. § 75-16); declaratory relief; attorneys' fees and costs (pursuant to N.C. Gen. Stat. § 75-16.1); and injunctive or other equitable relief.

COUNT VII
VIOLATIONS OF THE ARIZONA CONSUMER FRAUD ACT ("ACFA")
Ariz. Rev. Stat. § 44-1522, *et seq.*
(On Behalf of Plaintiffs and the Nationwide Class or, alternatively, the Arizona Subclass)

199. Plaintiffs fully incorporate by reference all of the above paragraphs, as though fully set forth herein.

200. The ACFA provides in pertinent part: "The act, use or employment by any person of any deception, deceptive or unfair act or practice, fraud, false pretense, false promise, misrepresentation, or concealment, suppression or omission of any material fact with intent that others rely on such concealment, suppression or omission, in connection with the sale or advertisement of any merchandise whether or not any person has in face been misled, deceived or damaged thereby, is declared to be an unlawful practice." Ariz. Rev. Stat. § 44-1522.

201. Plaintiffs and Class Members are "persons" as defined by Ariz. Rev. Stat. § 44-1521(6).

202. Defendants provides "services" as that term is included in the definition of "merchandise" under Ariz. Rev. Stat. § 44-1521(5), and Defendants are engaged in the "sale" of "merchandise" as defined by Ariz. Rev. Stat. § 44-1521(7).

203. Defendants engaged in deceptive and unfair acts and practices, misrepresentation, and the concealment, suppression and omission of material facts in connection with the sale and advertisement of "merchandise" (as defined in the ACFA) in violation of the ACFA, including but not limited to the following: (a) Failing to maintain sufficient security to keep Plaintiffs' and Class Members' confidential, financial, and personal data from being hacked and stolen; (b) Failing to disclose the Data Breach to Class Members in a timely and accurate manner, in violation of Ariz. Rev. Stat. § 18-552(B); (c) Misrepresenting material facts, pertaining to the sale of cryptocurrency wallets by representing that they would maintain adequate data privacy and security practices and

procedures to safeguard Class Members' PHI and PII from unauthorized disclosure, release, data breaches, and theft; (d) Misrepresenting material facts, in connection with the sale of cryptocurrency wallets by representing that they did and would comply with the requirements of relevant federal and state laws pertaining to the privacy and security of Class Members' PII; (e) Omitting, suppressing, and concealing the material fact of the inadequacy of the data privacy and security protections for Class Members' PII, (f) Engaging in unfair, unlawful, and deceptive acts and practices by failing to maintain the privacy and security of Class Members' PII, in violation of duties imposed by and public policies reflected in applicable federal and state laws, resulting in the Data Breach. These unfair, unlawful, and deceptive acts and practices violated duties imposed by laws, including Section 5 of the FTC Act; (g) Engaging in unlawful, unfair, and deceptive acts and practices by failing to disclose the Data Breach to Class Members in a timely and accurate manner; (h) Engaging in unlawful, unfair, and deceptive acts and practices by failing to take proper action following the Data Breach to enact adequate privacy and security measures and protect Class Members' PII from further unauthorized disclosure, release, data breaches, and theft.

204. The above unlawful, unfair, and deceptive acts and practices by Defendants were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury to Plaintiffs and Class Members that they could not reasonably avoid; this substantial injury outweighed any benefits to consumers or to competition.

205. Defendants knew or should have known that their computer systems and data security practices were inadequate to safeguard Class Members' PII and that risk of a data breach or theft was high. Defendants' actions in engaging in the above-named deceptive acts and practices were negligent, knowing and willful, and/or wanton and reckless with respect to the rights of Members of the Class.

206. As a direct and proximate result of Defendants' deceptive acts and practices, the Class Members suffered an ascertainable loss of money or property, real or personal, as described above, including the loss of their legally protected interest in the confidentiality of their PII.

207. Plaintiffs and Class Members seek relief under the ACFA including, but not limited to, injunctive relief, actual damages, treble damages for each willful or knowing violation, and attorneys' fees and costs.

COUNT VIII
Violations of the Kentucky Consumer Protection Act
Ky. Rev. Stat. §§ 367.110, et seq
(On Behalf of Plaintiffs and the Nationwide Class or, alternatively, the Kentucky Subclass)

208. Plaintiffs fully incorporate by reference all of the above paragraphs, as though fully set forth herein.

209. Plaintiffs and Kentucky Subclass Members purchased goods and services for personal, family, and/or household purposes from Defendants.

210. Defendants, operating in Kentucky, engaged in deceptive, unfair, and unlawful trade acts or practices in the conduct of trade or commerce, in violation of Ky. Rev. Stat. § 367.170, including but not limited to the following: (a) Fraudulently advertising material facts pertaining to its good and services to the Kentucky Subclass by representing and advertising that it would maintain adequate data privacy and security practices and procedures to safeguard Kentucky Subclass Members' Personal Information from unauthorized disclosure, release, data breaches, and theft; (b) Misrepresenting material facts pertaining to goods and services to the Kentucky Subclass by representing and advertising that it did and would comply with the requirements of relevant federal and state laws pertaining to the privacy and security of Kentucky Subclass Members' Personal Information; (c) Omitting, suppressing, and concealing the material fact of the inadequacy of the privacy and security protections for Kentucky Subclass Members' Personal

Information; (d) Engaging in deceptive, unfair, and unlawful trade acts or practices by failing to maintain the privacy and security of Kentucky Subclass Members' Personal Information, in violation of duties imposed by and public policies reflected in applicable federal and state laws, resulting in the Data Breach; (e) Engaging in deceptive, unfair, and unlawful trade acts or practices by failing to disclose the Data Breach to Kentucky Subclass Members in a timely and accurate manner, contrary to the duties imposed by Ky. Rev. Stat. § 365.732(2); and (f) Engaging in deceptive, unfair, and unlawful trade acts or practices by failing to take proper action following the Data Breach to enact adequate privacy and security measures and protect Kentucky Subclass Members' Personal Information from further unauthorized disclosure, release, data breaches, and theft.

211. As a direct and proximate result of Defendants' deceptive trade practices, Kentucky Subclass Members suffered an ascertainable loss of money or property, real or personal, as described above, including the loss of their legally protected interest in the confidentiality and privacy of their Personal Information.

212. The above unfair and deceptive practices and acts by Defendants were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury to Plaintiffs and Kentucky Subclass Members that they could not reasonably avoid; this substantial injury outweighed any benefits to consumers or to competition.

213. Defendants knew or should have known that its computer systems and data security practices were inadequate to safeguard Kentucky Subclass Members' Personal Information and that the risk of a data breach or theft was high. Defendants' actions in engaging in the above-named unfair practices and deceptive acts were negligent, knowing and willful, and/or wanton and reckless with respect to the rights of members of the Kentucky Subclass.

214. Plaintiff and Kentucky Subclass Members seek relief under Ky. Rev. Stat. § 367.220, including, but not limited to, damages, punitive damages, restitution and/or other equitable relief, injunctive relief, and/or attorneys' fees and costs.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, individually and on behalf of the other members of the Class proposed in this Complaint, respectfully request that the Court enter judgment in favor of Plaintiffs and the Class and against Defendants, as follows:

A. For an Order certifying this action as a class action and appointing Plaintiffs and their counsel to represent the Class;

B. For equitable relief enjoining Defendants from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiffs' and Class members' PII, and from failing to issue prompt, complete and accurate disclosures to Plaintiffs and Class members;

C. For equitable relief compelling Defendants to utilize appropriate methods and policies with respect to consumer data collection, storage, and safety, and to disclose with specificity the type of PII compromised during the Data Breach;

D. For equitable relief requiring restitution and disgorgement of the revenues wrongfully retained as a result of Defendants' wrongful conduct;

E. For an award of actual damages, compensatory damages, statutory damages, and statutory penalties, in an amount to be determined, as allowable by law;

G. For an award of punitive damages, as allowable by law;

H. For an award of attorneys' fees and costs, and any other expense, including expert witness fees;

I. Pre- and post-judgment interest on any amounts awarded; and

J. Such other and further relief as this court may deem just and proper.

JURY DEMAND

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

Dated: April 1, 2022

/s/ P. Bradford deLeeuw
P. Bradford deLeeuw (#3569)
DELEEUW LAW LLC
1301 Walnut Green Road
Wilmington, DE 19807
(302) 274-2180
(302) 351-6905 (fax)
brad@deleeuwlaw.com

OF COUNSEL:

Nicholas A. Migliaccio
Jason S. Rathod
MIGLIACCIO & RATHOD, LLP
412 H Street, NE, Suite 302
Washington, DC 20002
Phone: 202-470-520
Fax: 202-800-2730
nmigliaccio@classlawdc.com
jrathod@@classlawdc.com

JS 44 (Rev. 09/19)

CIVIL COVER SHEET

The JS 44 civil cover sheet and the information contained herein neither replace nor supplement the filing and service of pleadings or other papers as required by law, except as provided by local rules of court. This form, approved by the Judicial Conference of the United States in September 1974, is required for the use of the Clerk of Court for the purpose of initiating the civil docket sheet. *(SEE INSTRUCTIONS ON NEXT PAGE OF THIS FORM.)*

I. (a) PLAINTIFFS

Gregory Forsberg, Christopher Gunter, Samuel Kissinger, and Scott Sipprell

(b) County of Residence of First Listed Plaintiff Pima
(EXCEPT IN U.S. PLAINTIFF CASES)

(c) Attorneys *(Firm Name, Address, and Telephone Number)*

See attachment

DEFENDANTS

Shopify Holdings (USA), Inc., Shopify (USA) Inc., Shopify, Inc., and TaskUs, Inc.

County of Residence of First Listed Defendant New Castle
(IN U.S. PLAINTIFF CASES ONLY)

NOTE: IN LAND CONDEMNATION CASES, USE THE LOCATION OF THE TRACT OF LAND INVOLVED.

Attorneys *(If Known)*

II. BASIS OF JURISDICTION *(Place an "X" in One Box Only)*

- ❒ 1 U.S. Government Plaintiff
- ❒ 3 Federal Question *(U.S. Government Not a Party)*
- ❒ 2 U.S. Government Defendant
- ☒ 4 Diversity *(Indicate Citizenship of Parties in Item III)*

III. CITIZENSHIP OF PRINCIPAL PARTIES *(Place an "X" in One Box for Plaintiff and One Box for Defendant)*

(For Diversity Cases Only)

	PTF	DEF		PTF	DEF
Citizen of This State	❒ 1	❒ 1	Incorporated *or* Principal Place of Business In This State	❒ 4	❒ 4
Citizen of Another State	☒ 2	❒ 2	Incorporated *and* Principal Place of Business In Another State	❒ 5	❒ 5
Citizen or Subject of a Foreign Country	❒ 3	❒ 3	Foreign Nation	❒ 6	❒ 6

IV. NATURE OF SUIT *(Place an "X" in One Box Only)*

Click here for: Nature of Suit Code Descriptions.

CONTRACT	TORTS		FORFEITURE/PENALTY	BANKRUPTCY	OTHER STATUTES
❒ 110 Insurance	PERSONAL INJURY	PERSONAL INJURY	❒ 625 Drug Related Seizure of Property 21 USC 881	❒ 422 Appeal 28 USC 158	❒ 375 False Claims Act
❒ 120 Marine	❒ 310 Airplane	❒ 365 Personal Injury - Product Liability	❒ 690 Other	❒ 423 Withdrawal 28 USC 157	❒ 376 Qui Tam (31 USC 3729(a))
❒ 130 Miller Act	❒ 315 Airplane Product Liability	❒ 367 Health Care/ Pharmaceutical Personal Injury Product Liability		PROPERTY RIGHTS	❒ 400 State Reapportionment
❒ 140 Negotiable Instrument	❒ 320 Assault, Libel & Slander	❒ 368 Asbestos Personal Injury Product Liability		❒ 820 Copyrights	❒ 410 Antitrust
❒ 150 Recovery of Overpayment & Enforcement of Judgment	❒ 330 Federal Employers' Liability	PERSONAL PROPERTY	LABOR	❒ 830 Patent	❒ 430 Banks and Banking
❒ 151 Medicare Act	❒ 340 Marine	❒ 370 Other Fraud	❒ 710 Fair Labor Standards Act	❒ 835 Patent - Abbreviated New Drug Application	❒ 450 Commerce
❒ 152 Recovery of Defaulted Student Loans (Excludes Veterans)	❒ 345 Marine Product Liability	❒ 371 Truth in Lending	❒ 720 Labor/Management Relations	❒ 840 Trademark	❒ 460 Deportation
❒ 153 Recovery of Overpayment of Veteran's Benefits	❒ 350 Motor Vehicle	❒ 380 Other Personal Property Damage	❒ 740 Railway Labor Act	SOCIAL SECURITY	❒ 470 Racketeer Influenced and Corrupt Organizations
❒ 160 Stockholders' Suits	❒ 355 Motor Vehicle Product Liability	❒ 385 Property Damage Product Liability	❒ 751 Family and Medical Leave Act	❒ 861 HIA (1395ff)	❒ 480 Consumer Credit (15 USC 1681 or 1692)
❒ 190 Other Contract	☒ 360 Other Personal Injury		❒ 790 Other Labor Litigation	❒ 862 Black Lung (923)	❒ 485 Telephone Consumer Protection Act
❒ 195 Contract Product Liability	❒ 362 Personal Injury - Medical Malpractice		❒ 791 Employee Retirement Income Security Act	❒ 863 DIWC/DIWW (405(g))	❒ 490 Cable/Sat TV
❒ 196 Franchise				❒ 864 SSID Title XVI	❒ 850 Securities/Commodities/ Exchange
				❒ 865 RSI (405(g))	❒ 890 Other Statutory Actions
REAL PROPERTY	CIVIL RIGHTS	PRISONER PETITIONS	IMMIGRATION	FEDERAL TAX SUITS	❒ 891 Agricultural Acts
❒ 210 Land Condemnation	❒ 440 Other Civil Rights	Habeas Corpus:	❒ 462 Naturalization Application	❒ 870 Taxes (U.S. Plaintiff or Defendant)	❒ 893 Environmental Matters
❒ 220 Foreclosure	❒ 441 Voting	❒ 463 Alien Detainee	❒ 465 Other Immigration Actions	❒ 871 IRS—Third Party 26 USC 7609	❒ 895 Freedom of Information Act
❒ 230 Rent Lease & Ejectment	❒ 442 Employment	❒ 510 Motions to Vacate Sentence			❒ 896 Arbitration
❒ 240 Torts to Land	❒ 443 Housing/ Accommodations	❒ 530 General			❒ 899 Administrative Procedure Act/Review or Appeal of Agency Decision
❒ 245 Tort Product Liability	❒ 445 Amer. w/Disabilities - Employment	❒ 535 Death Penalty			❒ 950 Constitutionality of State Statutes
❒ 290 All Other Real Property	❒ 446 Amer. w/Disabilities - Other	Other:			
	❒ 448 Education	❒ 540 Mandamus & Other			
		❒ 550 Civil Rights			
		❒ 555 Prison Condition			
		❒ 560 Civil Detainee - Conditions of Confinement			

V. ORIGIN *(Place an "X" in One Box Only)*

☒ 1 Original Proceeding ❒ 2 Removed from State Court ❒ 3 Remanded from Appellate Court ❒ 4 Reinstated or Reopened ❒ 5 Transferred from Another District *(specify)* ❒ 6 Multidistrict Litigation - Transfer ❒ 8 Multidistrict Litigation - Direct File

VI. CAUSE OF ACTION

Cite the U.S. Civil Statute under which you are filing ***(Do not cite jurisdictional statutes unless diversity)***:
28 U.S. Code §1332(d)(2)

Brief description of cause:
Data breach class action

VII. REQUESTED IN COMPLAINT:

☒ CHECK IF THIS IS A **CLASS ACTION** UNDER RULE 23, F.R.Cv.P.

DEMAND $ In excess of 5 million

CHECK YES only if demanded in complaint:
JURY DEMAND: ☒ Yes ❒ No

VIII. RELATED CASE(S) IF ANY

(See instructions): JUDGE _____ DOCKET NUMBER _____

DATE 04/01/2022

SIGNATURE OF ATTORNEY OF RECORD /s/ P. Bradford deLeeuw

FOR OFFICE USE ONLY

RECEIPT # _____ AMOUNT _____ APPLYING IFP _____ JUDGE _____ MAG. JUDGE _____

ATTACHMENT

P. Bradford DeLeeuw
deLeeuw Law LLC 1301
Walnut Green Road
Wilmington, DE 19807
(302) 274-2180

Nicholas Migliaccio
Jason Rathod
Migliaccio & Rathod LLP
412 H St NE
Washington, DC 20002
(202) 470-3520