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.

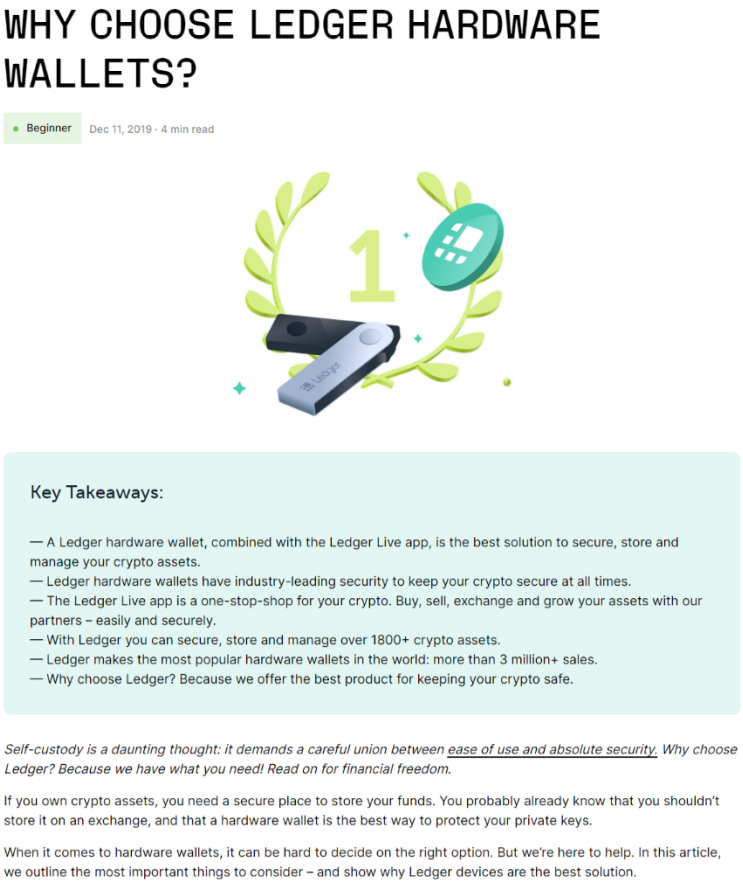
7. With their PII in hackers' hands, Plaintiffs and Class members are no longer in possession of a secure cryptocurrency portfolio.

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:

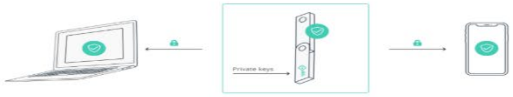
— Your crypto assets are completely intangible and exist solely on the blockchain
— How your handle your private keys for assets on the blockchain will define how secure those assets are
— Ledger hardware wallets allow you to store your keys within a device that is protected by Secure Element – a military 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.

DOCKET ALARM

Explore Litigation Insights

Docket Alarm provides insights to develop a more informed litigation strategy and the peace of mind of knowing you're on top of things.

Real-Time Litigation Alerts

Keep your litigation team up-to-date with **real-time alerts** and advanced team management tools built for the enterprise, all while greatly reducing PACER spend.

Our comprehensive service means we can handle Federal, State, and Administrative courts across the country.

Advanced Docket Research

With over 230 million records, Docket Alarm's cloud-native docket research platform finds what other services can't. Coverage includes Federal, State, plus PTAB, TTAB, ITC and NLRB decisions, all in one place.

Identify arguments that have been successful in the past with full text, pinpoint searching. Link to case law cited within any court document via Fastcase.

Analytics At Your Fingertips

Learn what happened the last time a particular judge, opposing counsel or company faced cases similar to yours.

Advanced out-of-the-box PTAB and TTAB analytics are always at your fingertips.

API

Docket Alarm offers a powerful API (application programming interface) to developers that want to integrate case filings into their apps.

LAW FIRMS
Build custom dashboards for your attorneys and clients with live data direct from the court.

Automate many repetitive legal tasks like conflict checks, document management, and marketing.

FINANCIAL INSTITUTIONS
Litigation and bankruptcy checks for companies and debtors.

E-DISCOVERY AND LEGAL VENDORS
Sync your system to PACER to automate legal marketing.