Regulating Risk without Custody: Lessons from the Trust Wallet Security Breach

Kenneth Achel[1]

ABSTRACT

On the eve of Christmas, Trust wallet released what appeared to be a routine update to the Trust Wallet Chrome browser extension (version 2.68) to fix bugs and improve some features.[2] This turned out to be their most problematic update yet. The update contained malicious code which was not part of the legitimate code released by the company. This malicious code was embedded with the purpose of stealing the seed phrase of Trust wallet users which will in turn give the hackers access to the crypto funds of the users who were attacked. Consequently, many crypto wallets were affected which resulted in the theft of about $7 million. While the company has pledged and is in the process of refunding the stolen funds to the affected victims, an updated version 2.69 was released promptly to mitigate the damage of the previous update. The CEO of Trust Wallet has also intimated publicly that an investigation is being conducted into the matter.[3] Although the company suffered considerable reputational damage, they seem to have salvaged the situation technically. However, this situation raises a critical legal and regulatory question which this paper seeks to address. The central question this paper will seek to address is whether or not non-custodial wallets such as Trust Wallet are legally liable for the funds of their users in the event of a breach.

---

[1] B.L Candidate 2026 (Ghana School of Law), LL.M International Trade and Business Law (Ghana Institute of Management and Public Administration), LL. B (Kwame Nkrumah University of Science and Technology).

[2] Trust Wallet, "Trust Wallet Browser Extension v2.68 Incident: An Update to Our Community," Trust Wallet Blog, December 29, 2025, <https://trustwallet.com/blog/announcements/trust-wallet-browser-extension-v268-incident-community-update> accessed 31 December 2025.

[3] Eowyn Chen (@EowynChen), X (formerly Twitter), December 26, 2025, <https://x.com/EowynChen/status/2004649284537647161> accessed 31 December 2025.

INTRODUCTION

Cryptocurrency has rapidly transitioned from a niche technology to a widely recognized and accepted component of modern financial life.[4] Many people[5], influenced by media coverage and personal networks, have begun acquiring cryptocurrency. Having purchased cryptocurrency, the next critical decision is secure storage, with non-custodial wallets emerging as a popular choice due to their emphasis on user sovereignty.[6]

Imagine the following scenario:

Your close friend who has been advocating for cryptocurrencies has tried to convince you several times to buy crypto because according to him "it's the next big thing." You were hesitant at first but after months of persistence you gave in to his request. You invested a substantial part of your savings into crypto. Your friend advised you to store your crypto in a 'non-custodial' wallet and you comply. One morning, you open your wallet to observe the growth of your investments when you discover that your funds are gone! Every single cent. What recourse do you have, and how does the law respond to such a loss?

This paper shall address these questions in the subsequent paragraphs.

CUSTODIAL AND NON – CUSTODIAL WALLETS

To address these questions, it is essential to understand the fundamental distinction between custodial and non-custodial wallets. Cryptocurrency transactions rely on a pair of cryptographic keys. The first is a private key which is a secret, randomly generated string that serves as proof of ownership and functions as a master password. A private key is commonly a 12-word phrase which the user keeps and uses to access their account and authorise transactions.

The second is a public key, and it is mathematically derived from the private key, which can be safely shared to receive funds or verify signatures. A hashed version of the public key generates the wallet address visible to others. The public key can be likened to a mobile

---

[4] Chainalysis Team, 'The Chainalysis 2025 Global Adoption Index' (*Chainalysis* 2 September 2025) <https://www.chainalysis.com/blog/2025-global-crypto-adoption-index>. accessed 2 January 2026.

[5] 'People' as used in this context refers to both natural and artificial persons.

[6] 'Non-Custodial Wallet Meaning | Ledger' (*Ledger* 4 October 2024) <https://www.ledger.com/academy/glossary/non-custodial-wallet> accessed 2 January 2026.

money number, a PayPal address, or Bank Account number which a party will send to another to receive funds therein. A shortened, hashed version of the public key becomes your wallet address (e.g., a Bitcoin address starting with "1" or "bc1"), which you share to receive funds.

The private key as the name suggests is private and is personal to the user as it is the only way they can access their account. A private key is like a bank vault's combination. Losing it means your funds are inaccessible forever. A public key however, can be shared to others for transacting. Losing a public key does not make the account inaccessible.

NON – CUSTODIAL WALLETS

Custodial wallets are fundamentally different from non – custodial wallets.

A non – custodial wallet gives its users full autonomy and sovereignty over their funds.[7] The users have exclusive access to their private keys and same is used to access their account or approve transactions. Under this model, crypto is not stored on the wallet provider's servers but is rather crypto is stored directly on the blockchain. The wallet provider merely provides a platform for their users to view and transfer their funds on. Accordingly, in the event that the wallet provider becomes insolvent or shuts down completely, users' funds still remain secure and accessible. This principle underpins the widely used phrase: "Not your keys, not your coins."[8]

CUSTODIAL WALLETS

This is vastly different from non-custodial wallets which are managed by a third – party[9] which stores users' crypto directly on their servers and keep its users' private keys. The users only have access to their public key. This arrangement offers convenience but introduces significant counterparty risk. If the custodian suffers a collapse or insolvency, users may permanently lose access to their funds. A quintessential example is the dramatic collapse of FTX in November 2022, where the assets of millions of users were effectively frozen or lost due to the exchange's mismanagement and insolvency.[10]

---

[7] Which fundamentally aligns with the core objective of cryptocurrency.

[8] Adam J Levitin, 'Not Your Keys, Not Your Coins: Unpriced Credit Risk in Cryptocurrency' [2022] SSRN Electronic Journal.

[9] Popularly known as centralized exchange.

[10] Nathan Reiff, 'The Collapse of FTX: What Went Wrong with the Crypto Exchange?' (*Investopedia* 10 October 2024) <https://www.investopedia.com/what-went-wrong-with-ftx-6828447> accessed 2 January 2026.

Trust Wallet is a company that operates the non-custodial wallet system. Therefore, they create an interface for their users to view and transact their crypto on but do not store your data on their servers. Trust wallet provides a private key comprising of a 12 – word seed phrase to their users upon the creation of their account. This seed phrase enables users to access their account and authorise transactions related to the said account. Thus, the only way a user's funds can be compromised is if a third party has access to their seed phrase. Not even hacking the company's server will give one access to the user's funds. This is why non-custodial wallets is preferred by most users.

So, what happened to trust wallet with the security breach was that it did not give the hackers access to the trust wallet server but it gave the hackers access to the seed phrase or private keys of the users. This enabled them steal funds from the trust wallet users.

ARE NON – CUSTODIAL WALLETS LEGALLY LIABLE FOR THE FUNDS OF THEIR USERS IN THE EVENT OF A SECURITY BREACH?

Generally, non – custodial wallets are absolved of liability in the event of loss of funds.[11] This is premised on the fact that the private keys of such wallets are the exclusive preserve of the users and as such, any risk associated with their funds are theirs.[12] Since the keys are kept by the user, the presumption is that if there is any security breach, it is the user's fault.

The difficulty comes however, when the loss of funds is not as a result of the users' negligence as was the case in the trust wallet scenario. There have been very few cases in this regard.

Notable among these is the case of *Meany et al v Atomic Wallet.*[13] This was a class action suit against Atomic Wallet, a decentralized non-custodial wallet. The plaintiffs' assets were stolen and same was attributed to North Korean hackers. The Plaintiffs based their claims on among others, negligence on the part of Atomic Wallet in their software design and security measures. Unfortunately, the court did not address the merit of the case but rather dismissed the action for want of jurisdiction[14]. According to the court, the Estonian based company did not have sufficient ties with the United States for a United States Court to have jurisdiction over it. The jurisdictional dismissals in this case highlight a significant challenge in crypto regulation and litigation. The borderless nature of crypto often shields international providers from accountability, leaving users in legal limbo.

---

[11] Legal Nodes Team, 'A Legal Guide to Custodial & Non-Custodial Wallets' (*Legalnodes.com*8 September 2022) <https://www.legalnodes.com/article/custodial-non-custodial-wallets> accessed 4 January 2026.

[12] Om Pal and others, 'Key Management for Blockchain Technology' (2019) 7 ICT Express 76.

[13] Civil Action No. 23-cv-01582-PAB-MEH.

[14] Ibid.

Another significant case in this regard is *Murphy et al. v. Phantom Technologies, Inc.* et al.[15] This case concerns a $500,000 theft, with plaintiffs alleging inter alia, that the app stored private keys in unencrypted browser memory. According to the plaintiffs, this act of negligence by the 1st defendant company led to the $500,000 theft. The case, filed in New York federal court, includes claims of negligence, fraud, and aiding money laundering. It is also quite unfortunate that this case has not been decided yet and still before the court. The conclusion of this matter will be authoritative and serve as a decisive locus classicus concerning the liability of non – custodial wallets in the event of security breaches.

Naturally, it is reasonable that due to the nature of decentralised non – custodial wallets, if a user is reckless with their private keys and same results in the loss of their funds, the company should not be liable. All major decentralized non-custodial wallets include broad liability disclaimers in their terms and conditions, absolving themselves from responsibility.[16] Some wallets take it a notch further to advise users not to save their seed phrases on their devices but to rather keep physical copies. As a result, certain wallets prevent users from taking screenshots of their private keys (or seed phrases) as an added security measure.[17]

However, where the loss of funds is occasioned by the negligence of the company, I hold the view that the company should be held liable. Typically, where there is negligence on the part of the company, a cause of action may lie.[18] However, it is important to note that the user must properly prove negligence. i.e., there was a duty owed by the company, the duty was breached, the breach caused damage to the user, and causation. It is very typical for legal claims regarding crypto theft to be dismissed where negligence is not proven.[19]

In my opinion, providers ought to owe a general duty of care to design, maintain, and update their software or hardware with reasonable security measures to prevent foreseeable harms, such as breaches exploiting known vulnerabilities. This ought to include:

---

[15] Case number 1:25-cv-03060

[16] See for example 'Terms of Service | Trust' (*Trust Website* 2024) <https://trustwallet.com/terms-of-service> accessed 4 January 2026.

[17] Trust Wallet, 'Lost Recovery Phase or Private Key' (*Trust Wallet Support*2025) <https://support.trustwallet.com/support/solutions/articles/67000734573-lost-recovery-phrase-or-private-key-how-to-protect-your-crypto> accessed 4 January 2026.

[18] 'Blockchain, Cryptocurrency and Non-Fungible Token Litigation Primer: A Tort Class Action - McGuireWoods' (*McGuireWoods* 9 October 2023) <https://www.mcguirewoods.com/client-resources/alerts/2022/3/blockchain-cryptocurrency-non-fungible-token-litigation-primer-ii/?referrer=grok.com> accessed 4 January 2026.

[19] See TERPIN V. AT&T MOBILITY LLC, No. 23-55375 (9th Cir. 2024); see also Fabian v. Lemahieu CASE NO. 4:19-cv-00054-YGR.

- Implementing audited cryptographic libraries, secure key generation/storage/usage protocols, and access controls (e.g., authentication, encryption, and isolation to avoid plaintext exposure).[20] They must ensure they are audited and safe so as to avoid key material leakage or complete loss of private keys.

- Wallets should require authentication. Wallet providers must ensure that they verify that users are who they say they are, and that only authorized parties can access the wallet's contents. The most common safeguards in non-custodial wallets are PIN codes, passphrases and biometrics. Added security measures such as two – factor authentication are highly recommended and should be made compulsory.

- Wallet providers also have the duty of being transparent after a breach through prompt notifications and cooperation in investigations.
- Wallet providers also owe contractual and representation – based duties. They must ensure that they fulfil the duties imposed on them in the terms incorporated in their contracts. They must also avoid misleading representations that imply breach-proof protection, which could lead to breach-of-contract or fraud claims. Accordingly, they must be very cautious in their marketing, website claims, app descriptions, and terms of service not to overpromise unbreakable, or absolute security. This is important because no system is truly "breach-proof" in the crypto world. Overpromising will entitle users to sue for breach of contract in the event of unavoidable breaches.
- Wallet providers must also ensure that they are data protection compliant. Accordingly, if a breach exposes user data, they owe duties under privacy laws like GDPR or CCPA to secure personal information.

On the other hand, there should be no duty against external cybercriminals, as causation is hard to prove if losses stem from user errors or sophisticated attacks. In Terpin v. AT&T Mobility LLC[21], a negligence claim failed due to insufficient causation details linking a breach to crypto theft.

Regulatory Context and Emerging Obligations

As of the time of publication of this paper, no global regulations specifically mandate security duties for pure non-custodial wallet providers, unlike custodial services under frameworks like the U.S. Bank Secrecy Act or EU's MiCA.

---

[20] Daniel Johnston, 'Custodial & Non-Custodial Digital Asset Wallet Risk Management' (*Forvis Mazars*3 March 2025) <https://www.forvismazars.us/forsights/2025/03/custodial-non-custodial-digital-asset-wallet-risk-management> accessed 4 January 2026.

[21] No. 23-55375 (9th Cir. 2024).

However, indirect impacts exist through the European Union's Markets in Crypto-Assets Regulation and Anti-Money Laundering Regulation[22] require Crypto-Asset Service Providers to conduct enhanced due diligence on interactions with non-custodial, "unhosted" wallets under the Travel Rule[23], focusing on AML/CFT[24] risks but not direct breach liability.

Trends in 2025-2026 emphasize consumer protections like risk disclosures and asset segregation for regulated entities, potentially influencing non-custodial standards via DeFi scrutiny.

In the U.S., bills like the Digital Asset Market Clarity Act 2025 and GENIUS Act focus on oversight but spare non-custodial tools from licensing if no control is exerted.

CONCLUSION

In the case of Trust Wallet, I do not consider the company negligent, as the recent breach emanated from a malicious update to their Chrome browser extension rather than any direct fault on their part. The incident appears to have been a sophisticated supply-chain attack exploiting the update process. Instead, Trust Wallet acted responsibly by quickly identifying the issue and releasing a patched version 2.69, promptly notifying users with clear warnings and instructions to secure their funds, and voluntarily committing to full reimbursement of verified losses

This proactive response demonstrates a commitment to user protection, even in a non-custodial model where users ultimately control their keys.

While we await the outcome of the ongoing U.S. lawsuit Murphy et al. v. Phantom Technologies Inc.,[25] it would be highly beneficial for multi-jurisdictional legislation to provide clearer guidelines and certainty on liability, best practices, and user protections in the decentralized wallet space.

Some stakeholders are advocating for mandatory cybersecurity and consumer protection standards for non-custodial services to prevent similar incidents. Others contend that such regulations could undermine the core purpose of non-custodial wallets; true self-

---

[22] Which will be applicable from 2027.

[23] European Parliament, 'Crypto-Assets: Green Light to New Rules for Tracing Transfers in the EU | News | European Parliament' (*www.europarl.europa.eu*20 April 2023) <https://www.europarl.europa.eu/news/en/press-room/20230414IPR80133/crypto-assets-green-light-to-new-rules-for-tracing-transfers-in-the-eu> accessed 5 January 2026.

[24] AML/CFT is an abbreviation for Anti-Money Laundering / Combating the Financing of Terrorism.

[25] Case number 1:25-cv-03060.

sovereignty, where users bear full responsibility without intermediary control. However, this regulatory debate is beyond the scope of this paper.