UNITED STATES DISTRICT COURT
DISTRICT OF COLORADO

ROBERT MEANY AND GRAHAM DICKINSON,

Plaintiffs,

v.

ATOMIC WALLET AND KONSTANTIN GLADYCH,

Defendants.

CASE NO.1:23-cv-1582

CLASS ACTION COMPLAINT AND DEMAND FOR JURY TRIAL

Plaintiffs file this Complaint on behalf of themselves, and all other similarly situated Atomic Wallet consumers, against Defendants Atomic Wallet and Konstantin Gladych.

INTRODUCTION

1. This is a class action brought on behalf of all persons who have suffered damages as a result of Defendants' negligent and unlawful conduct in connection with its cryptocurrency exchange platform, Atomic Wallet.

2. Plaintiffs in this case deposited cryptocurrency with Atomic Wallet, a decentralized "wallet" that accommodates various cryptocurrencies and is available to users on both a desktop and mobile application. Atomic Wallet is owned, designed, created, and advertised Defendants.

3. On or before June 3, 2023, countless Atomic Wallet user wallets around the world were hacked, resulting in the loss of over $100,000,000.00 (100 million) USD worth of

cryptocurrency related assets.

4. Defendants knew of existing security vulnerabilities in the Atomic Wallet platform since at least as early as 2022 but failed to take necessary security measures or precautions to protect user data and funds. Crypto research and security group Least Authority, who was hired by Defendants to evaluate Atomic Wallet's infrastructure, architecture, and design, issued a report in early 2022, advising Defendants of serious "exiting security vulnerabilities." Defendants were informed that funds held in Atomic Wallet may be at risk due to these security vulnerabilities but took no measures to inform users of those risks or protect against those risks. Least Authority highlighted security risks for Defendants, including but not limited to:

- current users are vulnerable to a range of attacks that may lead to the total loss of user funds, **specifically due to the current use and implementation of cryptography**;
- a lack of adherence to wallet system design and development standards and best practices;
- a lack of robust project documentation;
- an incorrect use of Electron, a framework for building desktop applications, leading to an **increased risk of potential security vulnerabilities** and implementation errors, as well as out-of-date and unmaintained dependencies.[1]

5. Despite knowledge of security vulnerabilities, and recommendations by consultants to assess those vulnerabilities and protect user assets, Defendants failed to implement reasonable safeguards. As a result, the Atomic Wallet platform was hacked and the Plaintiffs' funds stolen. Plaintiffs' wallets were vulnerable because of Defendants failure to implement security measures including those recommended by its own consulting security safety group and other measures that

[1] https://web.archive.org/web/20220210153123/https:/leastauthority.com/blog/disclosure-of-security-vulnerabilities-in-atomic-wallet/ (last accessed June 13, 2023) (emphasis added).

a reasonable company in the same industry should have implemented under the circumstances.

6. These additional security measures also include but are limited to: implementing security practices that prevent the installation of unauthorized software; and/or implementing company-wide training and education on best practices when performing job functions that have a potential to introduce vulnerabilities and/or unauthorized disclosure of private information or transfer of crypto assets.

7. As a result of Defendants' failures, over $100 Million in US Dollar equivalents were stolen from thousands users who used the Atomic Wallet platform.

PARTIES

I. Plaintiffs

8. Plaintiff Robert Meany is a citizen and resident of the State of Connecticut He is a natural person over the age of 21 and is otherwise *sui juris*. Plaintiff and class members, pursuant to contract with and solicitations from Defendants, purchased, repurchased, invested, and/or reinvested securities and held funds using the Atomic Wallet platform while in Connecticut. Plaintiff's transactions spanned from approximately May 14, 2021 through approximately June 3, 2023, at which point approximately $42,000 of Plaintiff's funds were stolen. As a result, Plaintiff sustained significant damages for which Defendants are liable.

9. Plaintiff Graham Dickinson is a citizen and resident of the State of Colorado. He is a natural person over the age of 21 and is otherwise *sui juris*. Plaintiff and class members, pursuant to contract with and solicitations from Defendants, purchased, repurchased, invested, and/or reinvested securities and held funds using the Atomic Wallet platform while in Connecticut. Plaintiff's transactions spanned from approximately 2021 through approximately 2023, at which point approximately $33,000 of Plaintiff's funds were stolen. As a result, Plaintiff sustained

significant damages for which Defendants are liable.

II. Defendants

10. Defendant Atomic Wallet was founded in 2017 as Atomic Swap by Konstantin Gladych. Atomic Swap was released in 2018. Upon information and belief, Mr. Gladych changed or reincorporated this corporate entity under the name Atomic Wallet, which is headquartered in Tallinn, Estonia. Atomic Wallet offers a platform for buying, selling, and trading securities, and holding funds, via a desktop and mobile application. It currently offers trading in over 500 crypto assets and makes available various other investment opportunities involving crypto assets, including a staking program. Atomic Wallet operates in multiple jurisdictions throughout the world including in Estonia, Nigeria, Russia, Iran, Turkey, Istabul, and Peru,[2] and is available to customers internationally and throughout the United States.

11. Defendant Konstantin Gladych is founder and CEO of Atomic Wallet, formerly Atomic Swap. Upon information and belief, Gladych is a citizen of Tallinn, Estonia who resides outside of the United States. Gladych launched Atomic Wallet in 2017 from Estonia and has since exercised complete control over all of Atomic Wallet's business activities at all times. Gladych is the sole executive at Atomic Wallet and answers to no board or shareholders. Gladych employs a "decentralized team" that works 100% remotely.[3]

JURISDICTION AND VENUE

12. This Court has subject matter jurisdiction over this action pursuant to 28 U.S. C. § 1332(d)(2) because this is a class action for a sum involving approximately $100,000,000 (100 million dollars), exclusive of interest and costs, in which at least one class member is a citizen of

[2] https://www.linkedin.com/company/atomicwallet/people/ (last accessed June 21, 2023).
[3] *See* https://atomicwallet.io/blog/christmas-greetings (last accessed June 21, 2023); https://atomicwallet.io/careers (last accessed June 21, 2023);

a state and Defendants are citizens of a foreign state.

13. Defendants are subject to personal jurisdiction in this District because they purposely availed themselves of the privilege of conducting activities in the United States and direct business activities toward, and conducts business with, consumers throughout the United States, including within the States of Colorado, Connecticut and all other States in the Union, through its website and mobile application, which is accessible to, marketed to, and used by United States investors. Furthermore, Defendants engaged in conduct that had a foreseeable, substantial effect in the United States connected with their unlawful acts.

14. Alternatively, Defendants are subject to personal jurisdiction in this District pursuant to Federal Rule of Civil Procedure 4(k)(2) because (i) Defendants are not subject to jurisdiction in any state's court of general jurisdiction; and (ii) exercising jurisdiction is consistent with the United States Constitution and laws.

15. Venue is proper in this District under 28 U.S. C. § 1391 because hundreds of Class Members reside in this District; Defendants engaged in business in this District; and Defendants entered into transactions and/or received substantial profits from Class Members who reside in this District.

FACTUAL ALLEGATIONS

I. Background on Cryptocurrency and the Products at Issue

16. A cryptocurrency is a form of digital asset based on a network that is distributed across many computers. At present, cryptocurrencies are not issued by central governments or authorities. Bitcoin is the most well-known cryptocurrency, but there are thousands of others. The value of some cryptocurrencies fluctuates with respect to the U.S. Dollar and all other fiat currencies. Other cryptocurrencies, like U.S. Dollar Coin, are so-called stablecoins because their value is pegged to a fiat currency-for U.S. Dollar Coin, the U.S. Dollar.

17. Different cryptocurrencies are typically designated by three-or four-letter symbols, like stock tickers. Bitcoin's is BTC. U.S. Dollar Coin is USDC. Coins at issue in this case include ETH, BZRX, OOKI, and several others.

18. The system by which a network of computers securely and publicly records the transactions of a given cryptocurrency is called a blockchain. There are several different blockchains that record transactions of a variety of different cryptocurrencies. The blockchains at issue in this case are called Ethereum, Polygon, and the Binance Smart Chain. Each of these blockchains has a "native" cryptocurrency, in which the computers operating the network are rewarded, and supports other cryptocurrency transactions as well. Ethereum's native cryptocurrency, for example, is Ether (ticker: ETH).

19. A cryptocurrency token is a unit of a specific virtual currency. These tokens are fungible and tradeable.

20. Cryptocurrency tokens are held via a virtual wallet. The wallet is secured using cryptography and can typically be accessed only with a lengthy passphrase, which is a form of strong password. The wallet has an address-typically a seemingly random of string of letters and numbers-that can be published on the blockchain without revealing the identity of the wallet-holder.

21. For cryptocurrency to reasonably function in a sophisticated marketplace, users must transact between currencies, crypto- or otherwise; must be able to lend and borrow; and must be able to earn some rate of return on stored assets.

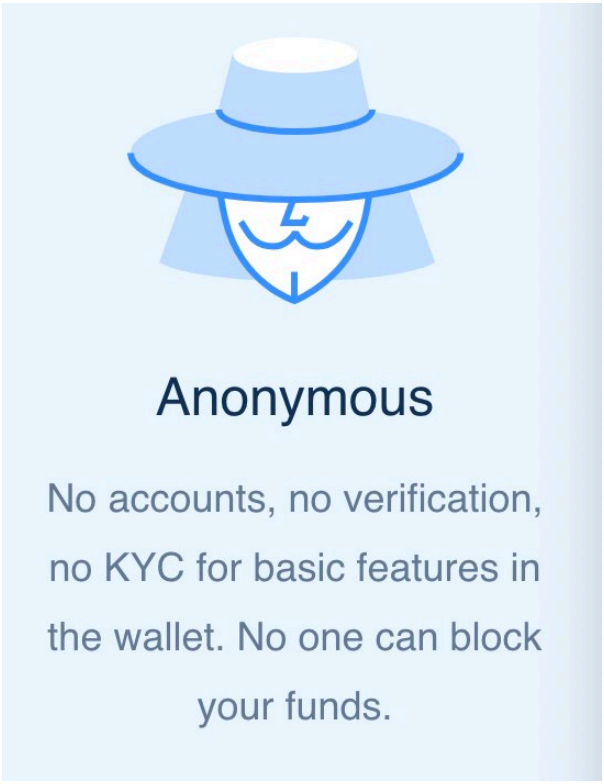
22. Equally important is that wallets in which these assets are stored must have an architecture and design, along with safety measures, which reasonably protect the stored assets from being compromised or hacked.

II. Atomic Wallet and its Promises

23. Atomic Wallet describes itself as a "non-centralized custodial" crypto wallet used "for buying, staking, & exchanging" that is "[t]rusted by 5,000,000 users worldwide."

24. Atomic Wallet represents that its platform is "secured" and promises users: "Your private keys are encrypted and never leave your device. You fully control your funds."

25. Atomic Wallet also touts that it does not employ verification or know-your-customer "KYC" controls:



26. Atomic Wallet's website describes its service as follows:

> Atomic Wallet is a non-custodial decentralized wallet. It means that you own your backup phrase and private keys, thus, you fully control your funds. We have no access to your wallet and your sensitive information. Your 12-words backup and private keys are stored locally on your device and strongly encrypted. Moreover, your funds are not located in the wallet itself, there are safely stored on the blockchain. Atomic Wallet connects directly to the blockchain nodes and shows the information about your balances, transaction history and everything you see in the wallet. It also allows you to perform transactions on the blockchain. Atomic

> Wallet also provides you with exchange and buying crypto services with the help of our partners.

27. The website further explains that user private keys and backup phrases are stored locally on user devices and "strongly encrypted" and that the wallet and all operations within it are password-protected. Atomic Wallet claims not to store any "private data" and claims that wallets are safe so long as users do not compromise their own devices or share their 12-wor backup or private keys. Atomic Wallet states on its website, "***Your backup is like a key to your wallet, whoever owns it, owns the funds. Take your passwords seriously***."

28. As set forth below, Atomic Wallet failed to take its own advice.

29. Atomic Wallet's failure to implement security measures, including those recommended by its own consulting security safety group, resulted in thousands of users' private keys being compromised by hackers in June 2023, resulting in over $100 million of losses to affected users.

30. The stolen funds appear at this point to be unrecoverable.

31. As set forth fully below, Defendants failed to take reasonable steps to secure the platform and prevent the theft that occurred as a result.

III. Defendants Were on Notice of Security Vulnerabilities on the Atomic Wallet Platforms but Failed to Inform Users of Relevant Risks and Failed to Mitigate Against Those Risks.

a. The Least Authority Audit Revealed Security Vulnerabilities and Recommended Action.

32. Approximately one year before Atomic Wallet user wallets around the world were hacked, resulting in over $100 million in lost cryptocurrency-related assets, Atomic Wallet hired crypto research and security group Least Authority to review, evaluate, and provide recommendations concerning Atomic Wallet's infrastructure.

33. In early 2022, Least Authority advised defendants of serious "existing security

vulnerabilities" impacting the security of user wallets and funds. Least Authority reported that users were vulnerable to a total loss of funds due to the current use and implementation of cryptography, a lack of adherence to wallet system best practices and standards, a lack of robust project documentation, and an incorrect use of Electron, a framework for building desktop apps.

34. In a published statement arising from its original audit and subsequent audits of Atomic Wallet, Least Authority stating in relevant part:

> [W]e strongly recommend that the Atomic Wallet team immediately notify users of the existing security vulnerabilities. In addition, until the issues and suggestions outlined in the report have been sufficiently remediated and the Atomic Wallet has undergone subsequent security audits, we strongly recommend against the Atomic Wallet's deployment and use.

35. Defendants did not undertake due diligence and remedial measures addressing vulnerabilities in its Atomic Wallet. Rather, Gladych responded with the following representations:

- We have taken all the issues discovered by Least Authority **into full account**.
- For some issues, we have already released corresponding patches and notified Least about doing so.
- To implement the remaining suggestions, **we will need to rework some parts of our application's core architecture. This will take some more time as per our estimate, but we are working on it. None of those issues pose any security risks to our users, as Atomic is a non-custodial wallet and all data is stored locally on users' devices**. We are **expecting to implement the rest of Least's suggestions in Q2 2022**. Once we are done, we will re-audit the application.
- Atomic Wallet has undergone two security audits so far. The other audit, conducted by DerSecur Ltd, asserted: "The application's average security score is 4.7. This result is higher than the market average. The application can be considered secure enough, nevertheless, we recommend bringing to the attention vulnerabilities discovered during the audit and consulting with the detailed results."
- Security is our highest priority, and we are continuously working on improving Atomic Wallet. Therefore, we have thoroughly reviewed Least's report and will be done

implementing their recommendations in full in Q2, 2022.[4]

36. Despite Defendants' promises and reassurances to customers of security, Atomic Wallet lacked reasonable safeguards and failed to implement measures to correct and mitigate against known security deficiencies. As a result, thousands of user wallets were hacked and the Plaintiffs' funds stolen. Plaintiffs' wallets were vulnerable because of Defendants failure to implement security measures including those recommended by its own consulting security safety group. Defendants knew the risks in their security systems, and the measures recommended to mitigate those risks as reasonably necessary to protect Plaintiffs' wallets from a hack. The end result was a total theft of over $100 Million in US Dollar equivalents.

b. In June 2023, Hackers Exploited Atomic Wallet's Known Security Vulnerabilities and Stole over $100 Million in US Dollar Equivalents.

37. On June 3, 2023, numerous sources began reporting an attack on Atomic Wallet that resulted in significant financial losses for many victims, including Plaintiffs in this action. According to Elliptic Connect ("Elliptic"), a blockchain analysis company, an estimated 5,500 crypto wallets have been affected by the attack, and losses have been reported at over $100 million. In many cases, users have lost entire portfolios.

38. On June 4, 2023 Atomic Wallet downplayed the hack on both its blog and its official Twitter account, reporting that "less than 1% of our monthly active users have been affected/reported," and that the "[s]ecurity investigation is ongoing" but has failed to provide any explanation as to the root cause of the losses.

39. Elliptic has traced stolen funds and linked them to the notorious Lazarus Group. Lazarus Group is a well-known and state-sponsored hacking group out of North Korea believed to

[4] Henken, *Least Authority Discloses Security Risks in Atomic Wallet* (Feb. 22, 2022), available at https://www.coindesk.com/tech/2022/02/10/least-authority-discloses-security-risks-in-atomic-wallet/ (last accessed June 21, 2023).

be responsible for stealing over $2 billion on crypto assets through various schemes. The U.S. FBI named Lazarus the prime suspect in a $100 million Harmony Protocol hack earlier this year. Lazarus is thus a known threat throughout the cryptocurrency marketplace.

40. The Elliptic investigation has revealed that the funds have been linked to a coin mixing service called Sinbad—the preferred mixer of Lazarus—and the funds are being swapped for bitcoin (BTC) before being laundered through Sinbad. Coin mixers enable anonymity in cryptocurrency transactions by randomly mixing crypto transfers to obscure the origin and destination of the funds.

41. Elliptic's analysts found that the Sinbad mixer was a clone of a different, previously-sanctioned mixer, Blender, and Lazarus had laundered over $100 million in stolen funds using Sinbad by February 2023.

42. Atomic Wallet has since taken down their download server, "get.atomicwallet.io," likely out of concern that their software was breached and to prevent the spread of further compromises.

43. Atomic Wallet is now collecting information from victims, asking what operating system they are using, where they downloaded the software, what was done before crypto was stolen, and where the backup phrase was stored. Victims are also asked to submit this information, and more, on a Google Docs "unauthorized transaction report" form[5] that was created to investigate the incident.

44. Based on the mass losses due to a single event hack, Defendants failed in providing sufficient security to prevent the hack which clearly infiltrated Defendants' servers and/or architecture of its Atomic Wallet design enabling the theft of Plaintiffs' and others similarly

[5] Available at https://docs.google.com/forms/d/1sSFm8VHKm-ifnjCGj-JA2godUWEOtV9tHVeI-DAaqVw/viewform?edit_requested=true.

situated assets and cryptocurrency property.

IV. Defendants Profits from Trade Fees.

45. Atomic Wallet charges customers fees for use of the platform, which represent Defendants' primary revenue source.

46. Atomic Wallet charges trade fees of 2-5%[6] for transactions involving fiat currency. In addition, the Atomic Website notes that the card's issuing bank will charge a processing fee that "can be quite high (around ~ 5%) as buying crypto purchases is seen as a high-risk operation."

47. Atomic Wallet charges all users a "network fee" for its "mining" services involved in processing transactions, including its Staking Service. The Atomic Wallet website states that the fee "goes to miners to process [the staking] transaction" and "the fee size depends on the network's current load. The more transactions are queued to get confirmed, the higher the fee will be." The website further states:

> Think about it this way: when making a transaction, you're the miners' client. Since any miner is always looking to increase their revenue, they'll first choose the transactions that offer the highest potential pay. When the network is overloaded and lots of transactions are queued to get completed, some people will be willing to offer higher fees to make their transactions more appealing to miners and thus speed up the confirmation process. Therefore, the average network fee will go up.

48. Atomic Wallet also charges a separate variable network fee for trades in BTC, LTC, and DGB, which changes depending on "the number of inputs" a single transaction will have. The website explains:

[6] While one section of the Atomic Wallet website states, "there is a flat 2% fee ($10 min) that you'll have to pay if you buy cryptocurrency with fiat," another section states, "Atomic Wallet charges a flat 5% fee, with a minimum of $10 per operation."

> What are inputs? Imagine you need to buy something that costs $350, and you need to pay with cash. Since a $350 bill doesn't exist, you'll use three $100 bills and one $50 bill. It will be quite easy for the cashier to count the money. If you use 35 $10 bills instead, though, things will get a bit harder.
>
> This works the same way on the blockchain. If Bob has 0.45 BTC on his balance, this amount is likely composed of numerous smaller BTC pieces. Instead of saying he owns 0.45 BTC, it would be more accurate to say he owns 0.1 + 0.2 + 0.1 + 0.05 BTC. Therefore, if he wanted to transfer 0.15 BTC to Alice, he'd be sending her 0.1 + 0.05 BTC, as opposed to a single 0.15 BTC piece.
>
> These 'pieces' are inputs. The more you're sending, the heavier the transaction will be.

49. Atomic Wallet charges a separate fee for trades in ETH, which reportedly "has no impact on the network fee size."

50. Atomic Wallet partners with exchanges and offers additional fees on those exchanges amounting to 0.5% plus the exchange partner commission.

CLASS ALLEGATIONS

51. As detailed below in the individual counts, Plaintiffs brings this lawsuit on behalf of themselves and all others similarly situated, pursuant to Rule 23(a), (b)(2), (b)(3), and/or (c)(4) of the Federal Rules of Civil Procedure.

I. Class Definitions

52. Plaintiffs seek to represent the following Global Class, Nationwide Class, and Colorado and Connecticut Subclass (collectively, the "Classes"):

(1) **Global Class:** All persons and entities residing outside of the United States who, within the applicable limitations period, purchased, repurchased, invested, and/or reinvested crypto assets on the Atomic Wallet platform and whose assets were stolen in June 2023.

(2) Nationwide Class: All persons or entities in the United States who, within the applicable limitations period, purchased, repurchased, invested, and/or reinvested crypto assets on the Atomic Wallet platform and whose assets were stolen in June 2023.

(3) Colorado Subclass: All persons or entities in the state of Colorado who, within the applicable limitations period, purchased, repurchased, invested, and/or reinvested crypto assets on the Atomic Wallet platform and whose assets were stolen in June 2023.

(4) Connecticut Subclass: All persons or entities in the state of Colorado who, within the applicable limitations period, purchased, repurchased, invested, and/or reinvested crypto assets on the Atomic Wallet platform and whose assets were stolen in June 2023.

Excluded from the Classes are Defendants and their officers, directors, affiliates, legal representatives, and employees; any governmental entities; and any judge, justice, or judicial officer presiding over this matter and the members of their immediate families and judicial staff.

53. The Class Period is January 1, 2017 through the present.

54. Plaintiffs reserve the right to modify or amend the definition of the proposed Classes, or to include additional classes or subclasses, if investigation or discovery indicate that the definitions should be narrowed, expanded, or otherwise modified, before or after the Court determines whether such certification is appropriate as discovery progresses.

II. Numerosity

55. The Classes are comprised of thousands of consumers globally, who used the Atomic Wallet platform and whose assets were stolen in June 2023. Membership in the Classes are thus so numerous that joinder of all members is impracticable. The precise number of class members is currently unknown to Plaintiffs but is easily identifiable through other means, such as through Atomic Wallet's corporate records or self-identification.

III. Commonality/Predominance

56. This action involves common questions of law and fact, which predominate over any questions affecting individual class members. These common legal and factual questions include, but are not limited to, the following:

(a) Whether Defendants owed a duty to Plaintiff and the Class;

(b) whether Defendants breached their duty to Plaintiff and the class;

(c) whether Defendants' actions were the proximate and actual cause of Plaintiffs' losses

(d) the type and measure of damages suffered by Plaintiffs and the Class;

(e) whether Plaintiffs and Class members have sustained monetary loss, and the measure of that loss;

(f) whether Plaintiffs and Class members are entitled to consequential damages, punitive damages, statutory damages, disgorgement, and/or other legal or equitable appropriate remedies as a result of Defendants' conduct.

IV. Typicality

57. Plaintiffs' claims are typical of the claims of the members of the Classes because all members were injured through the uniform misconduct in violation of laws described herein. Plaintiffs are advancing the same claims and legal theories on behalf of themselves and all such members. Plaintiff and members of the Class have sustained damages from Defendants' common course of unlawful conduct. Further, there are no defenses available to any Defendants that are unique to Plaintiffs.

V. Adequacy of Representation

58. Plaintiffs will fairly and adequately protect the interests of the members of the

Class. Plaintiffs have retained counsel experienced in complex consumer class action litigation, and Plaintiffs intend to prosecute this action vigorously. Plaintiffs have no adverse, conflicting, or antagonistic interests to those of the Classes. Plaintiffs anticipate no difficulty in the management of this litigation as a class action. To prosecute this case, Plaintiffs have chosen the undersigned law firms, which have the financial and legal resources to meet the substantial costs and legal issues associated with this type of consumer class litigation.

VI. Ascertainability

59. Members of the Class are readily ascertainable and identifiable. Members of the Class may be identified by blockchain ledger information and records maintained by Defendants or their agents.

VII. Requirements of Fed. R. Civ. P. 23(b)(3)

60. The questions of law or fact common to Plaintiffs' and each Class member's claims predominate over any questions of law or fact affecting only individual members of the Classes. All claims by Plaintiffs and the unnamed members of the Classes are based on the common course of conduct by Defendants.

61. Common issues predominate when, as here, liability can be determined on a class-wide basis, even when there will be some individualized damages determinations.

62. As a result, when determining whether common questions predominate, courts focus on the liability issue, and if the liability issue is common to the Classes as is in the case at bar, common questions will be held to predominate over individual questions.

a. Superiority

63. A class action is superior to individual actions for the proposed Classes, in part because of the non-exhaustive factors listed below:

(a) Joinder of all Class members would create extreme hardship and inconvenience for the affected customers as they reside worldwide, nationwide, and throughout the state;

(b) Individual claims by Class members are impracticable because the costs to pursue individual claims exceed the value of what any one Class member has at stake. As a result, individual Class members have no interest in prosecuting and controlling separate actions;

(c) There are no known individual Class members who are interested in individually controlling the prosecution of separate actions;

(d) The interests of justice will be well served by resolving the common disputes of potential Class members in one forum;

(e) Individual suits would not be cost effective or economically maintainable as individual actions; and

(f) The action is manageable as a class action.

VIII. Requirements of Fed. R. Civ. P. 23(c)(4)

64. As it is clear that one of the predominant issues regarding Defendants' liability is whether Defendants acted negligently, utilizing Rule 23(c)(4) to certify the Class for a class wide adjudication on this issue would materially advance the disposition of the litigation as a whole.

IX. Nature of Notice to the Proposed Class.

65. The names and addresses of all Class Members are contained in the business records maintained by Atomic Wallet and are readily available to Atomic Wallet. Alternative notice will be proposed in the form of electronic internet based NFTs and/or traditional internet-based communications and/or notices or advertisements. The Class Members are readily and objectively identifiable. Plaintiffs contemplate that notice will be provided to Class Members by e-mail, mail, and published notice.

COUNT 1
Negligence
(Plaintiffs Individually and on behalf of the Classes)

66. Plaintiffs repeat and re-allege the allegations contained in paragraphs 1-65 above, as if fully set forth herein.

67. Defendants owed Plaintiffs a duty to maintain the security of the funds in Atomic Wallet wallets, including but not limited to putting in place procedures such that a hacking attack would not result in a multi-million dollar theft; it breached that duty; and Defendants' actions in breaching their duty were the proximate and but-for cause of an injury-namely, the loss of funds deposited with Plaintiffs' Atomic Wallet wallets.

68. Defendants owed Plaintiffs a duty ensure that important passwords or security details could not be revealed to bad actors; it breached that duty; and Defendants' actions in breaching their duty were the proximate and but-for cause of an injury-namely, the loss of funds deposited with Plaintiffs' Atomic Wallet wallets.

69. Defendants owed Plaintiffs a duty secure against malicious attacks that could result in the theft of millions of dollars of assets; it breached that duty; and Defendants' actions in breaching their duty were the proximate and but-for cause of an injury-namely, the loss of funds deposited with Plaintiffs' Atomic Wallet wallets.

70. Defendants is therefore jointly and severally liable for Plaintiffs' injuries.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs pray for a judgment on behalf of themselves and the Classes:

a. Certifying the Classes as requested herein;

b. Awarding actual, direct and compensatory damages;

c. Punitive damages as appropriate

d. Awarding restitution and disgorgement of revenues if warranted;

e. Awarding alloable attorneys' fees and costs pursuant to Federal Rule of Civil Procedure 54, or any other applicable provision or principle of law; and

f. Providing such further relief as may be just and proper.

DEMAND FOR JURY TRIAL

Plaintiffs hereby demand a jury trial as to all claims so triable.

Dated: June 21, 2023

Respectfully submitted,

By: */s/ Douglass A. Kreis*
Douglass A. Kreis, Esq. (*pro hac vice* application forthcoming)
Daniel J. Thornburgh, Esq. (*pro hac vice* application forthcoming)
D. Nicole Guntner, Esq. (*pro hac vice* application forthcoming)
AYLSTOCK, WITKIN, KREIS & OVERHOLTZ
dkreis@awkolaw.com
dthornburgh@awkolaw.com
nguntner@awkolaw.com
17 East Main Street, Suite 200
Pensacola, FL 32502
Telephone: 850-202-1010
Fax: 850-916-7449

Counsel for Plaintiffs and the Class

ClassAction.org
