Trenton R. Kashima (SBN 291405)
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN PLLC
401 West Broadway, Suite 1760
San Diego, CA 91942
Tel.: (714) 651-8845
Email: tkashima@milberg.com

Attorneys for Plaintiffs and the Class

Additional Counsel Listed on Signature Page

UNITED STATES DISTRICT COURT

FOR THE NORTHERN DISTRICT OF CALIFORNIA

ALAN LEVINSON, individually and on behalf of themselves and all others similarly situated,

Plaintiff,

v.

INTUIT, INC. and ROCKET SCIENCE GROUP, LLC d/b/a Mailchimp, a Georgia Limited Liability Company,

Defendants.

Case No.

CLASS ACTION COMPLAINT FOR NEGLIENCE

JURY TRIAL DEMANDED

Plaintiff Alan Levinson ("Plainitff") alleges upon personal knowledge as to himself and his own actions, and upon information and belief, including the investigation of counsel as follows:

I. INTRODUCTION

1. Trezor Company s.r.o. and SatoshiLabs s.r.o. are Czech companies which sell an offline hardware cryptocurrency wallet called the "Trezor." Cryptocurrency wallets purportedly allow individuals to securely store their cryptocurrency until they sell or otherwise transfer it. The Trezor further provides an internet-based portal called the Trezor Suite, which allows users to access their cryptocurrency wallet and make transactions with cryptocurrency.

2. On the evening of April 2, 2022, users of the Trezor platform received a phishing email from malicious hackers who gained access to Trezors' customer email list (which included personal information, such as names, email addresses, IP addresses, etc.) negligently stored by Defendant Rocket Science Group, LLC, doing business as Mailchimp (hereinafter "Mailchimp"), to disseminate said phishing email stating, in relevant part, that their data had been compromised and that their cryptocurrency was "at risk of being stolen." The email itself was sent from "noreply@trezor.us." Mailchimp is a fully owned subsidiary of Defendant Intuit, Inc. ("Intuit"). All the information provided to Mailchimp, such as customer email lists, is maintained and secured on the "Intuit Platform."

3. This phishing email directed Trezor platform users to https://suite.trẹzor.com, a website URL that mirrored the Trezor platform's website https://trezor.io, to secure their account. Most people did not notice that there is an underdot under the letter "e" in "trẹzor" in that URL and that the link was leading them to a fake Trezor website. Once at this fake website, Trezor platform users would be prompted to download a new version of the Trezor Suite desktop application, in the process giving the hackers access to users' crypto wallets and most importantly, recovery seeds. Such credentials would give the hackers plenary control of a user's Trezor Suite account and the cryptocurrency contained within the offline wallets associated with these accounts.

4. The attack was reported by Trezor as "exceptional in its sophistication and ... clearly planned to a high level of detail," with the cloned version of the Trezor Suite app presenting a realistic functionality to anyone who installed it. Accordingly, Trezor platform users were unable to detect

the scam through reasonable means.

5. While the cyberattack on Plaintiff and Class Members was sophisticated, the attack on Defendants' computer systems and network that allowed the cybercriminals to access Plaintiff's and Class Members' information was not. Rather, Defendants fell victim to one of the oldest cybertricks in the book: according to reports, one of Defendants' employees fell victim to a phishing email and clicked on a malicious link.

6. Accordingly, the unknown hackers were able to pilfer Trezor platform users' cryptocurrency from the compromised accounts, resulting in millions of dollars of losses. By way of example, Plaintiff Levinson's cryptocurrency *was* stolen and, at the time of the theft, that cryptocurrency was valued at approximately $82,000.

7. The hacker's scheme was predicated on knowledge of the email addresses of the Trezor platform users. Here, the hackers gained the email addresses of the Trezor platform users by by compromising Trezor's services providers, Defendants Mailchimp and Intuit. Defendants were retained by Trezor to provide an opt-in newsletter to Trezor platform users. The hackers were able to access the Trezor email list (and likely other insensitive information) through Mailchimp and/or Intuit employee accounts. Indeed, Defendants confirmed that hackers used an internal employee tool to steal data from more than 100 of their clients — with the data being used to mount phishing attacks on the users of cryptocurrency services.

8. Defendants disregarded Plaintiff's and Class members' rights by intentionally, willfully, recklessly, or negligently failing to take adequate and reasonable measures to ensure that its data systems were protected, failing to take available steps to prevent and stop the breach from ever happening, and failing to disclose the breach of personal information in a timely manner. Plaintiff is informed and believes that Plaintiff's and Class members' personal information was improperly handled and stored and was not kept in accordance with applicable, required, and appropriate cyber-security protocols, policies, and procedures. As such, Plaintiff and the putative Class bring this Class Action to recover damages directly resulting from Defendants' laxed data security.

II. JURISDICTION AND VENUE

9. This Court has jurisdiction over the subject matter of this action pursuant to the Class Action Fairness Act. Defendant and members of the Class are residents of different states and Plaintiffs allege that the cumulative amount in controversy for Plaintiffs and the Class exceed $5 million, exclusive of interest and costs.

10. Personal jurisdiction exists over the Defendants because Defendants Intuit sells its services in the state of California, maintains a California Headquarters, and directs the actions of its subsidiaries (such as Mailchimp) from California.

11. Venue is proper in the Northern District of California because Intuit is headquartered in this District and the Defendants advertise and direct services into the stream of commerce from into this District.

12. This Action arises in Santa Clara County, where Intuit, Inc. is headquartered. Therefore, pursuant to Civil Local Rule 3-2(e), the appropriate divisional assignment is the San Jose Division

III. PARTIES

13. Plaintiff Alan Levinson is a citizen of Illinois who had his data compromised by the Defendants and was notified *via* email about the data breach alleged herein. Plaintiff had $87,000 stolen through the hackers' penetration of Defendants' systems and subsequent compromise of Plaintiff's information.

14. Defendant Rocket Science Group, LLC d/b/a Mailchimp is a subsidiary of Defendant Intuit, Inc. and is primarily located in Atlanta, Georgia. Mailchimp is an all-in-one Marketing Platform that provides email marketing service for other business.

15. Defendant Intuit, Inc. is headquartered in Mountain View, California. Intuit is a financial services and technology company and is the parent company of the "Intuit Group Companies," including Mailchimp, Credit Karma, Mint, Turbo Tax, and QuickBooks. Information collected by the Intuit Group Companies is secured and maintained by Intuit on its Intuit Platform.

IV. SUBSTANTIVE ALLEGATIONS

16. Trezor sells a hardware wallet capable of storing cryptocurrency called the "Trezor."

This cryptocurrency hardware wallet stores cryptocurrency offline to ensure security of users' cryptocurrency. The Trezor maintains an internet-based portal called the Trezor Suite, which allows users to access their cryptocurrency wallet and make transactions of cryptocurrency. Trezor Suite is accessible as a computer or mobile application.

17. To access the Trezor hardware wallet, users open the Trezor Suite. Additionally, when setting up a setting up a new Trezor Suite account, a 12 to 24-word recovery seed will be displayed that allows owners to recover their wallets if their device is stolen or lost. Anyone who knows this recovery seed can gain access to the wallet and its stored cryptocurrencies, making it vital to store the recovery seed in a safe place.

18. Mailchimp is subsidiary of Intuit or an "Intuit Group Company." Intuit makes it clear that is aggerates and hosts the email addresses collected by Mailchimp on its "Intuit Platform." Indeed, Intuit's privacy policy states the following:

> Our [Intuit] Platform is designed to help you connect with other people and organizations. As a result of those connections, others may be able to input information about you, including business customers using the Intuit Platform. For example, one of Intuit's customers may share information about you with us in order to use and benefit from the Intuit Platform, such as information relevant to your or other customer contacts' interactions with a business that is using Mailchimp.

Intuit's privacy policy continues to state.

> When we say "platform" we mean that when you choose to share data with us, or bring over information from third parties (like a bank or loan provider), we use that data together, not just within the individual offering(s) you're using. This means that, for example, your bookkeeping details from QuickBooks, budgets from Mint, contact and purchase history details from Mailchimp, and recommendations from Credit Karma all live together.
>
> The personal information we use in this centralized way is all the information that Intuit knows about you, either because you are an end user of our services or a customer contact (like a subscriber to a customer's email list) whose personal information has been included in the Intuit Platform. It includes information such as your credentials; your name and contact details; payment information; information about your activities, behavior, your interests and preferences (including purchase history with Intuit or if you're a customer contact, our customers); insights about your finances, business or preferences or your contacts; the content you or others place about you in our Platform; and information we have collected about you from third-party sources.

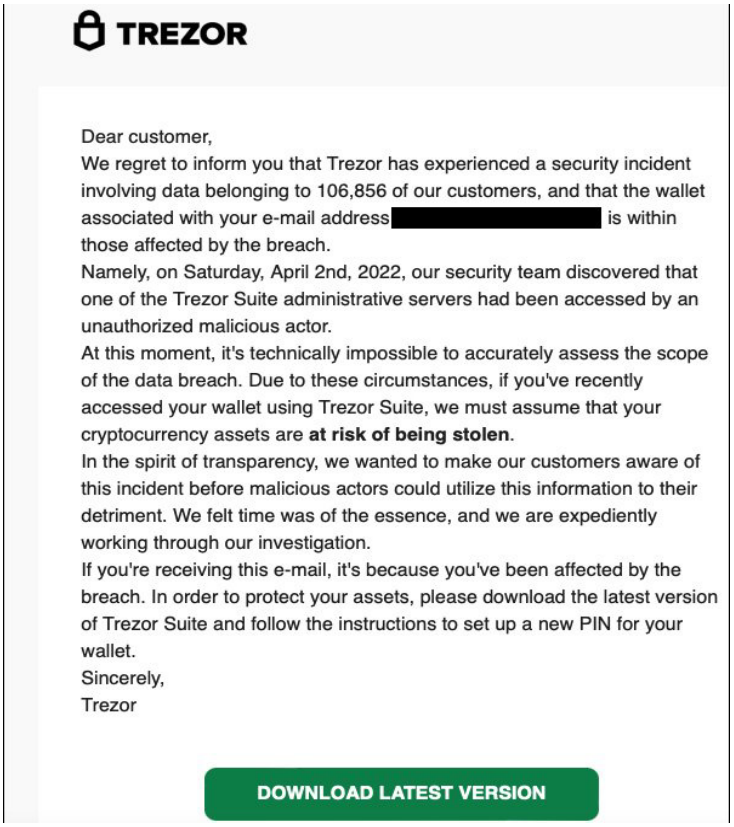
Put more simply, any consumer contact information provided to an Intuit Group Company (such as email addresses provided to Mailchimp) is provided to Intuit. This is not surprising as the data

collected by Intuit Group Companies is extremely valuable when aggregated.

19. In the process of collecting all this information, including the customer lists of Trezor which contained Plaintiff's and Class Members' contact information, Defendants assumed the duty of protecting said information.

20. In April of 2022, Defendants' computer systems and network were infiltrated and accessed by unauthorized criminals. According to reports, the hackers gained unauthorized access to Defendants' employees email accounts through a run of the mill phishing scheme whereby one of the employees clicked on a malicious link in an email. Once inside these email accounts, the hackers gained access to a tool used by the Mailchimp's customer support and account administration teams to access information on the Intuit Platform. The hackers were then able to view around 300 Mailchimp user accounts and obtain audience data (i.e. email and other personal information) from 102 of them. One of these user accounts was Trezor.

21. On the evening of April 2, 2022, the hackers who compromised the Intuit Platform sent out the following email to Trezor platform users:



TREZOR

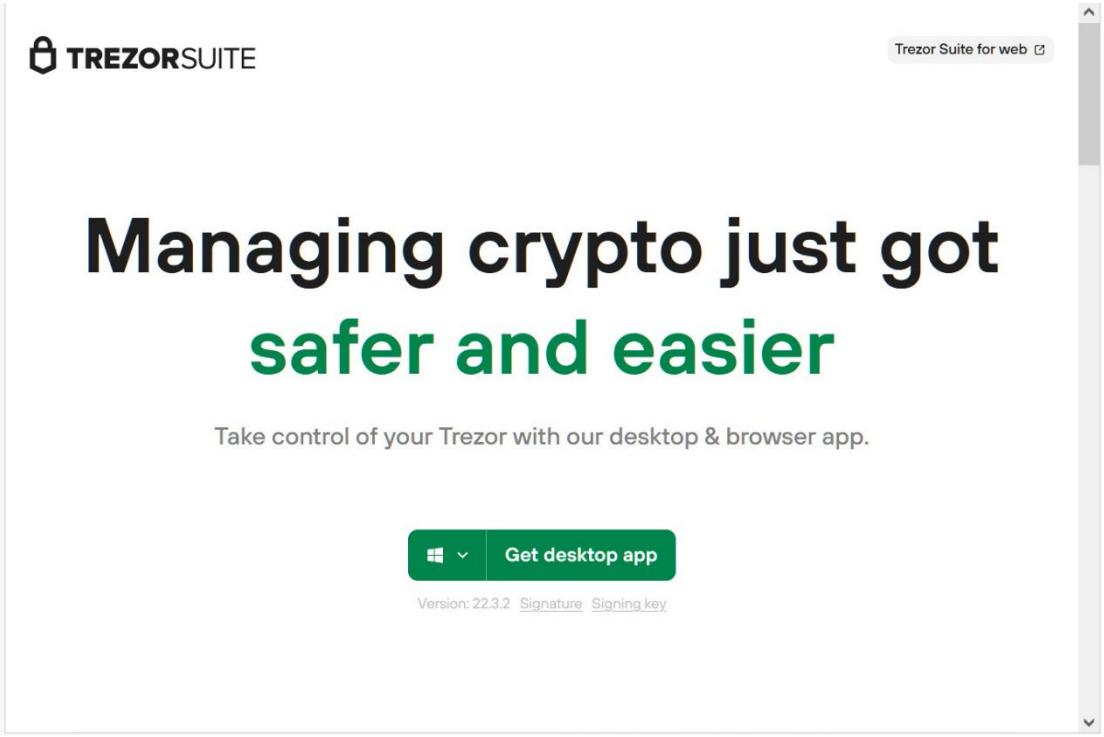
Dear customer,
We regret to inform you that Trezor has experienced a security incident involving data belonging to 106,856 of our customers, and that the wallet associated with your e-mail address [redacted] is within those affected by the breach.
Namely, on Saturday, April 2nd, 2022, our security team discovered that one of the Trezor Suite administrative servers had been accessed by an unauthorized malicious actor.
At this moment, it's technically impossible to accurately assess the scope of the data breach. Due to these circumstances, if you've recently accessed your wallet using Trezor Suite, we must assume that your cryptocurrency assets are **at risk of being stolen**.
In the spirit of transparency, we wanted to make our customers aware of this incident before malicious actors could utilize this information to their detriment. We felt time was of the essence, and we are expediently working through our investigation.
If you're receiving this e-mail, it's because you've been affected by the breach. In order to protect your assets, please download the latest version of Trezor Suite and follow the instructions to set up a new PIN for your wallet.
Sincerely,
Trezor

DOWNLOAD LATEST VERSION

This email appeared to come from Trezor and was only directed at Trezor platform users.

22. If a person clicked the "download" link contained with the email, they would be taken to a phishing website that appears in the browser as "suite.trẹzor.com." However, the website is a domain name using Punycode characters that allows the attackers to impersonate the trezor.com domain using accented characters. But to a reasonable person, it would appear that they were being directed to a Trezor domain.

23. This phishing website prompts users to download the updated Trezor Suite application:



This phishing website mirrors the look of Trezor's actual website; again, preventing a reasonable consumer from understanding the scam. When a visitor downloads the application linked on the phishing website, a fake version of the Trezor Suite application was downloaded.

24. Once the Trezor platform user connects their Trezor wallet to the fake Trezor Suite app, it will prompt them to enter their 12 to 24-word recovery phrase, which is sent back to the hackers. This recovery phrase is meant to allow Trezor platform users the ability to recover lost wallets, but in the hands of the hackers it allows unauthorized parties to import the recovery phrase into their own wallets and steal victims' cryptocurrency assets.

25. But what made this phishing attack successful was that the Hackers could target Trezor platform users directly, by emailing known email accounts associated with actual Trezor users.

26. On April 14, 2022, Trezor sent the following email to its customers notifying them of the breach:

> **Details of the Mailchimp data breach**
> This email contains details of a data breach which compromised our mailingprovider between February and April 2, 2022.
>
> The attack saw Mailchimp employees being phished for privileged access to customer accounts, resulting in the theft of email addresses and in some cases names of subscribers and other data.
>
> Below you will find specific data belonging to you which was stolen in the attack.
>
> **Data stolen in the attack**
> Your email address
> Your IP address
> An approximate location based on your internet provider[1]
>
> Please use this information to protect yourself and be wary of any incoming mail, as the targeted data is being used to send phishing emails to your inbox. Avoid clicking on any links in emails, and never ever enter your seed into a computer without your Trezor device telling you to do so.
>
> This is the latest information we have, following a week of investigation and reluctant cooperation from Mailchimp's senior security staff. You will find a timeline of events on Trezor blog, but we will not be providing any links here so this message does not get confused for a phishing attempt.
>
> For inquiries, please contact our security team at security@satoshilabs.com.
>
> You will not receive any more emails from Trezor via Mailchimp. Given the broad scope of the attack, it is important that you remain on alert for phishing attacks coming from other sources, as hundreds of other brands and projects which have not yet been disclosed were also targeted.

27. Trezor noted that Defendants were not cooperative in resolving and responding to this breach:

> We are most surprised by the lack of transparency and cooperation from Mailchimp regarding the attacks. We received one email to a catch-all support email about "possible risks" but did not learn of these attacks until we discovered the leak and started pushing for answers. Now that we have access to the affected customer data, it is clear that not only were subscriber email addresses stolen, but also data of people who unsubscribed, and in some cases names and IP addresses.

By Defendants' own admission, they knew of the data breach on March 26, 2022, a week before the

[1] Collectively, this information is referred to herein as the personally identifiable information or "PII".

phishing emails were sent. Accordingly, Defendants had advance notice of the breach, knew it was possible, if not likely, Plaintiff and Class Members were at risk, but did nothing to inform Plaintiff and Class Members of the risks associated therewith (even though Defendants had email addresses for Plaintiff and the Class). It was only after Trezor pressed Defendants that any alarm was raised.

28. This lack of action was particularly concerning, as Defendants acknowledged that the hackers targeted customers in the cryptocurrency and finance sectors and that the hackers gained access to API keys for an undisclosed number of customers, allowing the attackers to send phishing emails. Accordingly, Defendants were well aware that the hackers were likely to conduct a phishing attack of the type described herein.

29. Defendants negligently and unlawfully failed to safeguard Plaintiff's and Class Members' personal data by allowing cyberthieves to access information contained on Defendants' Intuit Platform. Accordingly, as outlined below, Plaintiff and Class Members now have lost valuable cryptocurrency and remain at a greater risk of other online fraud.

30. Indeed, Plaintiff Levinson is and was a user of Trezor to store his cryptocurrency. Prior to the data breach, Plaintiff Levinson had at least $87,000 worth of cryptocurrency stored on his Trezor cryptocurrency wallet.

31. Then, on or about April 2, 2022, Plaintiff Levinson received the phishing email described herein. His email address and the fact that he was a Trezor customer was only known to the hackers due to Defendants' negligence. Plaintiff Levinson was convinced by the authentic looking phishing email and believed that the best way to protect his cryptocurrency would be to click a link embedded within the phishing email to help "secure" his cryptocurrency. Then, on the fake landing page, Plaintiff was prompted to enter codes which gave hackers access to his cryptocurrency.

32. As a result, Plaintiff had $87,000 worth of cryptocurrency stolen from his Trezor wallet. As such, Plaintiff has suffered harm in the form of loss property, loss of time, frustration, and other harm due to the Defendants' inadequate cybersecurity protocols, procedures, and policies.

33. Even worse, Defendants failed to announce in a timely manner that their cybersecurity systems had been compromised and this, in turn, also harmed Plaintiff who could have been saved

from exposing himself through the phishing email's duplicitous design made possible by Defendants' failures.

The Data Breach was a Foreseeable Risk of which Defendant was on Notice

35. In 2021, there were a record 1,862 data breaches last year, surpassing both 2020's total of 1,108 and the previous record of 1,506 set in 2017.[2]

36. In light of recent high profile data breaches at other industry leading companies, including, Microsoft (250 million records, December 2019), Wattpad (268 million records, June 2020), Facebook (267 million users, April 2020), Estee Lauder (440 million records, January 2020), Whisper (900 million records, March 2020), and Advanced Info Service (8.3 billion records, May 2020), Defendants knew or should have known that their electronic records would be targeted by cybercriminals.

37. Indeed, cyberattacks have become so notorious that the FBI and U.S. Secret Service have issued a warning to potential targets so they are aware of, and prepared for, a potential attack.

38. Despite the prevalence of public announcements of data breach and data security compromises, and despite its own acknowledgments of data security compromises, and despite its own acknowledgment of its duties to keep PII private and secure, Defendants failed to take appropriate steps to protect the PII of Plaintiff and the proposed Class from being compromised.

At All Relevant Times Defendants Had a Duty to Plaintiff and Class Members to Properly Secure their Private Information

39. At all relevant times, Defendants had a duty to Plaintiffs and Class Members to properly secure their PII, encrypt and maintain such information using industry standard methods, train its employees, utilize available technology to defend its systems from invasion, act reasonably to prevent foreseeable harm to Plaintiff and Class Members, and to promptly notify Plaintiff and

[2] https://www.cnet.com/tech/services-and-software/record-number-of-data-breaches-reported-in-2021-new-report-says/.

Class Members when Defendants became aware that their PII may have been compromised.

40. Defendants' duty to use reasonable security measures arose as a result of the relationship that existed between Defendants, on the one hand, and Trezor, on the other hand.

41. Defendants' duty to use reasonable security measures also arose as a result of Defendants voluntarily assumption of Plaintiff's and Class Member's PII.

42. Defendants had the resources necessary to prevent the data breach but neglected to adequately invest in security measures, despite its obligation to protect such information. Accordingly, Defendants breached their common law, statutory, and other duties owed to Plaintiff and Class Members.

43. Security standards commonly accepted among businesses that store PII using the internet include, without limitation:

a. Maintaining a secure firewall configuration;

b. Maintaining appropriate design, systems, and controls to limit user access to certain information as necessary;

c. Monitoring for suspicious or irregular traffic to servers;

d. Monitoring for suspicious credentials used to access servers;

e. Monitoring for suspicious or irregular activity by known users;

f. Monitoring for suspicious or unknown users;

g. Monitoring for suspicious or irregular server requests;

h. Monitoring for server requests for PII;

i. Monitoring for server requests from VPNs; and

j. Monitoring for server requests from Tor exit nodes.

44. The ramifications of Defendants' failure to keep its consumers' PII secure are long lasting and severe. Once PII is stolen, fraudulent use of that information and damage to victims may

continue for years.

***Defendants* Failed to Comply with FTC Guidelines**

45. Federal and State governments have likewise established security standards and issued recommendations to temper data breaches and the resulting harm to consumers and financial institutions. The Federal Trade Commission ("FTC") has issued numerous guides for business highlighting the importance of reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.[3]

46. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established guidelines for fundamental data security principles and practices for business.[4] The guidelines note businesses should protect the personal consumer and consumer information that they keep, as well as properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct security problems.

47. The FTC recommends that companies verify that third-party service providers have implemented reasonable security measures.[5]

48. The FTC recommends that businesses:

a. Identify all connections to the computers where you store sensitive information.

b. Assess the vulnerability of each connection to commonly known or reasonably foreseeable attacks.

c. Do not store sensitive consumer data on any computer with an internet connection unless it is essential for conducting their business.

[3] Federal Trade Commission, *Start With Security, available at*: https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf

[4] Federal Trade Commission, *Protecting Personal Information: A Guide for Business, available at*: https://www.ftc.gov/tips-advice/business-center/guidance/protecting-personal-information-guide-business

[5] FTC, *Start With Security*, *supra* note 18.

d. Scan computers on their network to identify and profile the operating system and open network services. If services are not needed, they should be disabled to prevent hacks or other potential security problems. For example, if email service or an internet connection is not necessary on a certain computer, a business should consider closing the ports to those services on that computer to prevent unauthorized access to that machine.

e. Pay particular attention to the security of their web applications—the software used to give information to visitors to their websites and to retrieve information from them. Web applications may be particularly vulnerable to a variety of hack attacks

f. Use a firewall to protect their computers from hacker attacks while it is connected to a network, especially the internet.

g. Determine whether a border firewall should be installed where the business's network connects to the internet. A border firewall separates the network from the internet and may prevent an attacker from gaining access to a computer on the network where sensitive information is stored. Set access controls—settings that determine which devices and traffic get through the firewall—to allow only trusted devices with a legitimate business need to access the network. Since the protection a firewall provides is only as effective as its access controls, they should be reviewed periodically.

h. Monitor incoming traffic for signs that someone is trying to hack in. Keep an eye out for activity from new users, multiple log-in attempts from unknown users or computers, and higher-than-average traffic at unusual times of the day.

i. Monitor outgoing traffic for signs of a data breach. Watch for unexpectedly large amounts of data being transmitted from their system to an unknown user. If large amounts of information are being transmitted from a business' network, the transmission should be investigated to make sure it is authorized.

49. The FTC has brought enforcement actions against businesses for failing to protect consumer and consumer data adequately and reasonably, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

50. Because Defendants voluntarily assumed Plaintiff's and Class Members' PII, Defendants had a duty to the Class Members to keep their PII secure.

51. Defendants were at all times fully aware of their obligation to protect the PII of Plaintiff and Class Members. Defendants were also aware of the significant repercussions if they failed to do so.

52. Defendants' failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

Defendant Fails to Comply with Industry Standards

53. Several best practices have been identified that at a minimum should be implemented by companies like Defendants, including but not limited to: educating all employees; strong passwords; multi-layer security, including firewalls, anti-virus, and anti- malware software; encryption, making data unreadable without a key; multi-factor authentication; backup data; and limiting which employees can access sensitive data.

54. Other best cybersecurity practices that are standard in the healthcare industry include installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches and routers; monitoring and protection of physical security systems; protection against any possible communication system; and training staff regarding critical points.

55. Defendant failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

56. These foregoing frameworks are existing and applicable industry standards in the Defendants' industry, and Defendants failed to comply with these accepted standards, thereby opening the door to and causing the Data Breach.

57. At all relevant times, Defendant knew, or reasonably should have known, of the importance of safeguarding the data of Plaintiff and Class Members and of the foreseeable consequences that would occur if Defendant's data security system and network was breached, including, specifically, the significant costs that would be imposed on Plaintiff and Class Members as a result of a breach.

58. Defendant knew or should have known about these dangers and strengthened its data, IT, and email handling systems accordingly. Defendant was put on notice of the substantial and foreseeable risk of harm from a data breach, yet it failed to properly prepare for that risk.

V. CLASS ACTION ALLEGATIONS

59. Plaintiff brings this action as a class action pursuant to Federal Rule of Civil Procedure 23(a) and 23(b)(3) for the following Class of persons under breach of contract and breach of the implied covenant of good faith and fair dealing:

> All persons residing in the United States who received the unauthorized April 2, 2022 Trezor branded email purportedly informing them of a data security incident and who lost cryptocurrency as a result thereof.

Excluded from the Class are Defendant's officers, directors, and employees; any entity in which Defendant has a controlling interest; and the affiliates, legal representatives, attorneys, successors, heirs, and assigns of Defendants. Also excluded from the Class are members of the judiciary to whom this case is assigned, their families and Members of their staff.

60. Numerosity. The Members of the Class are so numerous that joinder of all of them is impracticable. While the exact number of Class Members is unknown to Plaintiff at this time, based on information and belief, the Class consists of over 100 individuals. All members of the proposed Class are readily ascertainable as the email address are known to Defendants and can be matched to Trezor accounts.

61. Commonality. There are questions of law and fact common to the Class, which predominate over any questions affecting only individual Class Members. These common questions of law and fact include, without limitation:

a. Whether any Defendant owed a due to Plaintiff and the Class;
b. Whether any Defendant negligently used, maintained, lost, or disclosed Plaintiff's and Class Members' personal information;
c. Whether any Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the data breach;
d. Whether any Defendant's data security systems prior to, during, and after the data breach complied with the applicable data security standards;
e. Whether any Defendant breached a duty to Class Members to safeguard their personal information;
f. Whether the Defendants knew or should have known that their data security systems and monitoring processes were deficient;
g. Whether the Plaintiff and Class Members suffered legally cognizable injuries as a result of the Defendants' actions or inaction;
h. Whether Plaintiff and Class Members are entitled to damages and/or injunctive relief.

62. Typicality. Plaintiff's claims are typical of those of other Class Members because Plaintiff's information, like that of every other Class Member, was compromised in the data breach.

63. Adequacy of Representation. Plaintiff will fairly and adequately represent and protect the interests of the Members of the Class. Plaintiff's Counsel are competent and experienced in litigating Class actions.

64. Predominance. Defendants have engaged in a common course of conduct toward

Plaintiff and Class Members, in that all of Plaintiff's and Class Members' data was stored on the same computer system and unlawfully accessed in the same way. The common issues arising from Defendant's conduct affecting Class Members set out above predominate over any individualized issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

65. Superiority. A Class action is superior to other available methods for the fair and efficient adjudication of the controversy. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a Class action, most Class Members would likely find that the cost of litigating their individual claims is prohibitively high and would therefore have no effective remedy. The prosecution of separate actions by individual Class Members would create a risk of inconsistent or varying adjudications with respect to individual Class Members, which would establish incompatible standards of conduct for Defendants. In contrast, the conduct of this action as a Class action presents far fewer management difficulties, conserves judicial resources and the parties' resources, and protects the rights of each Class Member.

66. Defendants have acted on grounds that apply generally to the Class as a whole, so that Class certification, injunctive relief, and corresponding declaratory relief are appropriate on a Class-wide basis.

VI. CAUSES OF ACTION

COUNT ONE
NEGLIGENCE
(On Behalf of the Class)

67. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully alleged herein.

68. Defendants collected non-public personal information from Plaintiff and other Class Members to provide services on behalf of Trezor. In doing so, Defendants undertook contractual obligations and otherwise voluntarily assumed a duty to protect that PII.

69. Defendants knew or should have known that the information that it collected regarding Plaintiff and other Class Members was sensitive, and breach of such data would lead to significant financial loss.

70. By collecting and storing this data, and sharing it and using it for commercial gain, Defendants had a duty of care to use reasonable means to secure and safeguard this information, to prevent disclosure of the information, to guard the information from theft, and inform individuals of any data breach.

71. Defendants' duty included a responsibility to implement a process by which it could detect a breach of its security systems in a reasonably expeditious period of time and give prompt notice to those affected in the case of a data breach.

72. Defendants also owed a duty of care to Plaintiffs and members of the Class to provide security consistent with industry standards, and to ensure that its systems and networks and the personnel responsible for them adequately protected their customers' information.

73. Only Defendants were in a position to ensure that its systems were sufficient to protect against the harm to Plaintiff and the members of the Class from a data breach. Defendants breached their duties by failing to use reasonable measures to protect Plaintiff's and Class Members' personal information.

74. The specific negligent acts and omissions committed by Defendants include, but are not limited to, the following:

a. failing to adopt, implement, and maintain adequate security measures to safeguard Plaintiff's and Class Members' personal information;
b. failing to adequately monitor the security of its networks and systems;
c. allowing unauthorized access to Plaintiff's and Class Members' personal information; and
d. failing to recognize in a timely manner that Plaintiff's and other Class Members' personal information had been compromised.

75. It was foreseeable that Defendants' failure to use reasonable measures to protect and monitor the security of Plaintiff's and other Class Members' personal information would result in injury to Plaintiff and other Class Members. Indeed, Defendants knew that it was providing services to a company that provides cryptocurrency wallets to consumers. Cryptocurrency wallets are specifically designed to protect valuable cryptocurrency. Additionally, Defendants aggregate significant amounts of personal data, including financial data, in its databases. Any secure breach of such information would be highly likely to lead to the exact type of phishing scam described herein.

76. It was therefore foreseeable that the failure to adequately safeguard personal

information would result in one or more of the following injuries to Plaintiff and the members of the proposed Class: economic harm due to successful and potentially ongoing phishing attacks; ongoing, imminent, certainly impending threat of identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; loss of the confidentiality of the stolen confidential data; the illegal sale of the compromised data on the deep web black market; expenses and/or time spent on credit monitoring and identity theft insurance; time spent scrutinizing bank statements, credit card statements, and credit reports; expenses and/or time spent initiating fraud alerts; decreased credit scores and ratings; lost work time; and other economic and non-economic harm.

77. As a result of this misconduct by Defendants, the personal information of Plaintiffs and the Class were compromised, resulting in the loss of property (including cryptocurrency) and placing them at a greater risk of identity theft and subjecting them to actual identity theft. Plaintiffs and the Class have also suffered consequential out of pocket losses for procuring credit freeze or protection services, identity theft monitoring, and other expenses relating to identity theft losses or protective measures.

COUNT TWO
BREACH OF THID PARTY BENEFICIARY CONTRACT
(On Behalf of the Class)

78. Plaintiff fully incorporates by reference all of the above paragraphs, as though fully set forth herein.

79. Plaintiff brings this claim for breach of third-party beneficiary contract against Defendants.

80. Defendants entered into a contract to provide customer services to Trezor.

81. The contracts were made expressly for the benefit of Plaintiff and the Class, as it was their PII that Defendants agreed to collect and protect through its services. Thus, the benefit of collection and protection of the PII belonging to Plaintiff and the Class was the direct and primary objective of the contracting parties.

82. Defendants knew that if they were to breach these contracts with their customers, the customers' clients, including Plaintiff and the Class, would be harmed by, among other harms, fraudulent transactions.

83. Defendants breached their contracts with Trezor when it failed to use reasonable data security measures that could have prevented the Data Breach.

84. As foreseen, Plaintiff and the Class were harmed by Defendants' failure to use reasonable security measures to store the PII of Plaintiff and the Class, including but not limited to the risk of harm through the loss of their PII.

85. Accordingly, Plaintiff and the Class are entitled to damages in an amount to be determined at trial.

COUNT THREE
UNJUST ENRICHMENT
(On Behalf of the Class)

86. Plaintiff re-alleges and incorporates by reference paragraphs 1-85 above as if fully set forth herein.

87. Plaintiff alleges this claim in the alternative to Count 2 above.

88. Plaintiff and Class Members conferred a monetary benefit on Defendant in the form of their PII.

89. Defendant collected, maintained, and stored the PII of Plaintiff and Class Members and, as such, Defendant had knowledge of the monetary benefits conferred by them.

90. The money that Defendant received from Plaintiff's and Class Members' PII should have been used to pay, at least in part, for the administrative costs and implementation of data security adequate to safeguard and protect the confidentiality of Plaintiff's and Class Members' PII.

91. Defendant failed to implement—or adequately implement—those data security practices, procedures, and programs to secure sensitive PII, as evidenced by the data breach.

92. As a result of Defendant's failure to implement data security practices, procedures, and programs to secure sensitive PII, Plaintiff and Class Members suffered actual damages in an

amount of the savings and costs Defendant reasonably and contractually should have expended on data security measures to secure Plaintiffs' PII.

93. Under principles of equity and good conscience, Defendant should not be permitted to retain the money it received from Plaintiff's and Class Members' PII that should have been used to implement the data security measures necessary to safeguard and protect the confidentiality of Plaintiff's and Class Members' PII.

94. As a direct and proximate result of Defendant's decision to profit rather than provide adequate security, and Defendant's resultant disclosures of Plaintiff's and Class Members' PII, Plaintiff and Class Members suffered and continue to suffer considerable injuries in the forms of time and expenses mitigating harms, diminished value of PII, loss of privacy, and a present increased risk of harm.

VI. PRAYER FOR RELIEF

WHEREFORE, Plaintiff and members of the Class pray for relief and judgment as follows:

A. For an order declaring that this action is properly maintained as a class action and certifying a class representative(s) in accordance with Rule 23 of the Federal Rules of Civil Procedure, appointing Plaintiff as representative for the Class, and appointing Plaintiff's counsel as Class counsel;

B. Ordering Defendants to pay for not less than three years of credit monitoring services for Plaintiff and the Class;

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

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

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

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

G. All such other and further relief as this court may deem just and proper.

VII. JURY TRIAL DEMAND

Plaintiff demands a trial by jury for all of the claims asserted in this Complaint so triable.

Respectfully submitted,

DATED: April 22, 2022

s/ Trenton R. Kashima
Trenton R. Kashima (SBN 291405)
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN PLLC
401 West Broadway, Suite 1760
San Diego, CA 91942
Tel.: (714) 651-8845
Email: tkashima@milberg.com

Nick Suciu III*
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN PLLC
6905 Telegraph Rd., Suite 115
Bloomfield Hills, MI 48301
Tel.: (313) 303-3472
Fax: (865) 522-0049
Email: nsuciu@milberg.com

Gary M. Klinger*
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN PLLC
227 W. Monroe Street, Suite 2100
Chicago, IL 60606
Tel.: (866) 252-0878
Email: gklinger@milberg.com

Attorneys for Plaintiffs and the Classes

**Pro Hac Vice forthcoming*