

UNITED STATES DISTRICT COURT  
DISTRICT OF NEW JERSEY

MANDAR MIRASHI,

Plaintiff,

v.

JOHN DOE,

An unknown individual(s),

v.

521.99931468 Bitcoin,

*In rem* Defendant,

v.

FixedFloat, Kraken, ChangeNow, exch.cx, TradeOgre, and John Doe 2,

Relief Defendants.

Case. No.

COMPLAINT FOR DAMAGES AND  
EQUITABLE RELIEF PURSUANT TO:

1. The Computer Fraud and Abuse Act, 18 U.S.C. §1030 *et seq.*;
2. The New Jersey Computer-Related Offenses Act, NJSA 2A:38A *et seq.*;
3. Common Law Fraud;
4. Common Law Conversion of Property;
5. Replevin under NJSA 2B:50-1
6. Common Law Unjust Enrichment; and
7. Equitable Relief, Including
  - (a) Freeze and Disgorgement of Stolen Assets;
  - (b) Accounting
  - (c) Establishment of Constructive Trust
  - (d) Freeze of John Doe's Assets

Plaintiff Mandar Mirashi brings this case against fictitious defendant John Doe by and through his attorneys, upon personal knowledge as to his own conduct, and upon information and belief as to the conduct of others, as follows:

**INTRODUCTION**

1. Plaintiff Mandar Mirashi is the victim of cryptocurrency theft. On February 27, 2025 an unknown hacker stole \$40 million in Bitcoin from his cryptocurrency wallets.

2. John Doe, whose identity is unknown, used fraudulent tactics including falsified communications from Google, Ledger, and other parties to access Plaintiff's computer.

3. Once John Doe had access to Plaintiff's computer, John Doe drained Plaintiff's cryptocurrency wallets of over \$40 million of Bitcoin and other assets.

4. Plaintiff is now tracking his assets across the bitcoin blockchain and requests an order freezing his Stolen Assets, an order freezing the assets of the hacker where such assets can

be identified, an order instructing certain virtual asset service providers (VASPs) to provide information on the identity of the hacker and transactions involving the Stolen Assets, and other relief.

### **PARTIES**

5. Plaintiff Mandar Mirashi is an individual who resides in Hudson County, New Jersey.

6. John Doe is the unknown hacker who illegally accessed Mr. Mirashi's computer and cryptocurrency wallets and stole Mr. Mirashi's Bitcoin. Plaintiff does not know John Doe's location.

7. *In rem* defendant 521.99931468 Bitcoin is the Bitcoin that was stolen from Mr. Mirashi by John Doe.

8. Relief Defendant FixedFloat is a virtual asset service providers (VASP) that received deposits of the Stolen Assets. FixedFloat is a Delaware corporation.

9. Relief Defendant Kraken is a VASP that received deposits of the Stolen Assets. Kraken is headquartered in Canada.

10. Relief Defendant ChangeNow is a VASP that received deposits of the Stolen Assets. ChangeNow is headquartered in the Seychelles.

11. Relief Defendant exch.cx is a VASP that received deposits of the Stolen Assets. Exch.cx is registered in Belize.

12. Relief Defendant TradeOgre is a VASP that received deposits of the Stolen Assets. On information and belief, TradeOgre is headquartered in the United States.

13. The "John Doe 2" Relief Defendant is one or more unknown cryptocurrency exchanges that have received 45 deposits of Mr. Mirashi's Bitcoin.

### **JURISDICTION AND VENUE**

14. This Court has subject matter jurisdiction over this lawsuit pursuant to 28 U.S.C. §1331 because this case involves a federal question under the Computer Fraud and Abuse Act (18 U.S.C. §1030 *et seq.*).

15. This Court has personal jurisdiction because defendant John Doe committed an intentional tort; Plaintiff suffered the harm from the tort in New Jersey; and John Doe directed his fraudulent conduct at New Jersey.

16. Venue is appropriate in this District because Plaintiff Mandar Mirashi is a resident of this District and the cause of action arose in this District. Plaintiff accessed his wallets and conducted the transactions referred to herein from his computer in Hudson County, New Jersey.

## **FACTUAL ALLEGATIONS**

### **Plaintiff's Ownership and Custody of the Stolen Assets**

17. As of February 27, 2025 Plaintiff maintained two cryptocurrency wallets containing digital assets including 521.99931468 Bitcoin (the “Stolen Assets”).

18. Cryptocurrency wallets, like bank accounts, have identifying numbers called addresses but are otherwise anonymous.

19. Plaintiff's wallets bear the addresses:

36cfw3QiQeJJryX7JbWb1DKL7ZP1zMuF1S (“Plaintiff Wallet 1”) and  
33oV5phadHeUPEgjVNH9fVUZsNhAeDLhAN (“Plaintiff Wallet 2”).

20. Plaintiff's wallets are located on the bitcoin blockchain, a publicly available cryptocurrency ledger which records transactions conducted using the cryptocurrency Bitcoin. The cryptocurrency Bitcoin, as opposed to the bitcoin blockchain, is referred to as “BTC.”

### **The Phishing Attempts**

21. The attempt to steal Mr. Mirashi's BTC began on February 25, 2025 at 4:01 p.m. when Mr. Mirashi received from an email from Google Workspace Alerts informing him that he was dead.

22. The email stated that there was a legal matter involving Mr. Mirashi's Google account and provided a case number.

Alert: Reporting rule - [ACTION REQUIRED] There is a legal matter involving your Google Account ➤ [Inbox](#)

Google Workspace Alerts <google-workspace-alerts-noreply@google.com>  
to me

Tue, Feb 25, 4:01 PM (4 days ago) [star](#) [Reply](#) [Details](#)

## Google Workspace

This Reporting rule alert is to inform you that specific activity occurred based on a custom reporting rule.

The alert details include:

- Date: Tue, Feb 25 2025 21:01 UTC
- Rule Name: [ACTION REQUIRED] There is a legal matter involving your Google Account - Assigned to Avery S ([post-mortem-cases@google.com](#)) Case ID: 8827813310511809

##- Please type all replies inside the case file -##

You are receiving this notice because your email address is linked to the Google Account referenced in your request. We extend our deepest sympathies to you during this difficult time and appreciate your patience. If you have any questions or wish to provide additional information, you can access the case using the authorized email address provided below. For your privacy, sensitive details have been redacted from this email, which will be permanently deleted within 30 days. If you did not make this request, you may cancel it at any time through the case.

Case file: <https://sites.google.com/u/8827813310511809/d/1mC6lg4plfUONle1ltlBnmBH23ltuC/edit>

Full name of the deceased person: [redacted] [redacted]

Email address of the deceased person: \*\*\*\*\*@\*\*\*\*\*.\*\*

Full name of relative/legal representative: [redacted] [redacted]

Email address of relative/legal representative: \*\*\*\*\*@\*\*\*\*\*.\*\*

Attachments: social\_scan.pdf, proof\_of\_address.pdf, court\_certified\_letters\_testamentary.pdf, passport\_scan.pdf, death\_cert\_(2).pdf

Additional comments or instructions: Please forward all replies to my protonmail, thanks. Tim.

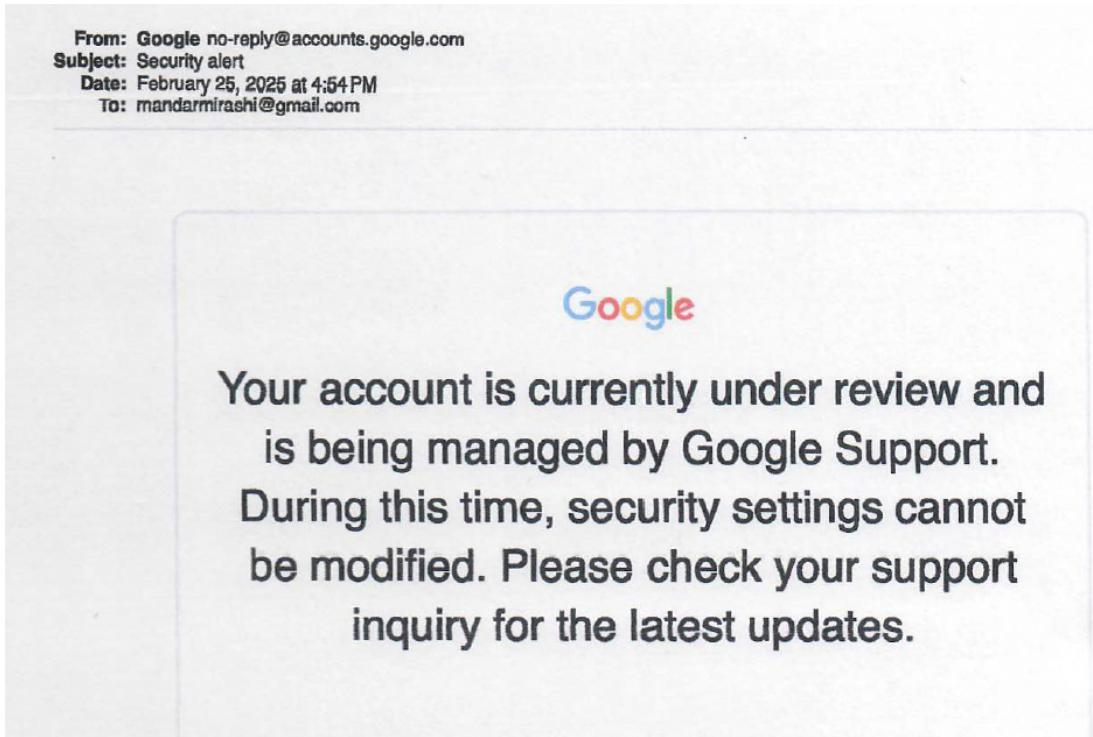
23. Mr. Mirashi clicked on the “Case File” link provided in the email, signed into his Google account, and learned that Google believed he was dead.

24. Mr. Mirashi knew that Google has a procedure for relatives of a deceased Google customer to retrieve the deceased’s emails, documents, and other materials.

25. Later, however, Mr. Mirashi thought it was strange that such an email would be sent to him, the party listed as deceased.

26. Mr. Mirashi immediately contacted Google and told Google that he suspected he was being hacked.

27. Google froze Mr. Mirashi’s security settings and asked him to cancel the case that was opened, which he did.



28. Mr. Mirashi also maintains several “cold storage” or “hardware” wallets manufactured by Ledger SAS, a Paris-based company.

29. These wallets are small devices designed to store a user’s private keys, which are the passwords used to access cryptocurrency assets.

30. If a fraudster obtains a user’s private keys, the fraudster can control the user’s cryptocurrency wallets and assets.

31. At 8:31 p.m. Mr. Mirashi received an email from support+recover@ledger.com, which appeared to be from Ledger.

32. The email’s line was “Attention Required: Ledger Recover Initiated.” The email contained the device IDs of Mr. Mirashi’s three Ledger devices as well as his date of birth and the last four digits of his social security number:

**From:** support-recover@ledger.com  
**mandarmirashi@gmail.com**  
**Subject:** Attention Required: Ledger Recover Initiated  
**Date:** February 25, 2025 at 8:31 PM  
**To:** Mandar Mirashi mandarmirashi@gmail.com

**LEDGER** 

Dear Mandar,

**Ledger Recover has been initiated for your device(s)**

You are receiving this notice due to your recovery request through Ledger Recover on 12:36 AM - February, Wednesday 26th, 2025 UTC. If you did not initiate this recovery process, immediate action is required.

This is in regards to the Ledger customer:

Name: MANDAR X. MIRASHI  
Address: 36 Duncan Ave, Jersey City, NJ 07304, USA  
Date of Birth: \*\*-\*\*-1970  
SSN: \*\*\*-\*\*-5467

**Devices in Recovery Request**

Ledger LGR-9H2F-7T4K-1X8P  
Ledger LGR-5R3M-6Q9S-2V5W  
Ledger LGR-8B4N-1Z6D-3Y7C

**Verification Documents Submitted**

**Government ID** Driver's License  
**Onfido Status** Identity verification submitted and pending review

**Want to cancel this request?**

**Offline Device Usage:** The verification tool can be used on an air-gapped device for your security.

**Instructions to use the verification tool:**

1. Get the latest version from the link below
2. Open it on your device of choice
3. Generate your extended public key
4. Copy the xPub (extended public key) from the tool
5. **Reply directly to this email with your xPub keys, and say you would like to cancel this request**

Ensure you provide your xPub for each device mentioned in your request.

Providing your xPub is the fastest way to verify your identity.

**Ledger xPub offline tool**

Only the original device owner can provide the correct public keys

**Important:** Simply reply to this email with your xPub keys to expedite the verification process.

Our team will process your request within the next 24 hours. We thank you for your patience during this matter.

Stay secure,  
The Ledger Recover Team

This is an automated security alert

© Ledger SAS. All rights reserved. Ledger, Ledger Stax, Ledger Nano S, Ledger Vault, Bolos are trademarks owned by Ledger SAS. | 106 rue du Temple, 75003 Paris, France

33. Mr. Mirashi knew that Ledger offered a service called “Ledger Recover,” but he had not subscribed to it.

34. The email also referred to an identity verification procedure where Mr. Mirashi’s drivers’ license would have to be reviewed. The email also provided a link asking for Mr. Mirashi’s extended public key.

35. Mr. Mirashi suspected the email was a phishing attempt and contacted Ledger at 9:32 p.m. informing Ledger that he was not a subscriber and that he believed he was the target of a phishing scam.

**From:** Mandar Mirashi mandarmirashi@gmail.com  
**Subject:** Re: Attention Required: Ledger Recover Initiated  
**Date:** February 25, 2025 at 9:32 PM  
**To:** phishing@ledger.com, care@ledger.fr, support@onfido.com

Ledger support - I do not subscribe to ledger recover. It looks like I am a target of a phishing scam.

They have obtained my address and other information and looks like they are trying to hack my account

They claim to also have sent my drivers license to Onfido for verification so I am also copying Onfido for awareness.

Please follow up.

36. At 9:33 p.m. Mr. Mirashi received a form response from Ledger.

37. At 9:34 p.m. Mr. Mirashi received an email from care@ledger.fr stating that his case had been closed due to inactivity. The email also invited him to click on a link to open a new ticket.

38. At 10:03 p.m. Mr. Mirashi received an email from care@ledger.fr asking for the phone number or email of the people who contacted Mr. Mirashi so they could be reported to the authorities.

39. At 10:19 p.m. Mr. Mirashi responded stating that he had already sent the original phishing email to Ledger.

**From:** Mandar Mirashi [mandarmirashi@gmail.com](mailto:mandarmirashi@gmail.com)  
**Subject:** Re: Ledger Support - Case 00113667 [thread::MX3iR-Mxcgm7AhDy8HSPbyi::]  
**Date:** February 25, 2025 at 10:19 PM  
**To:** Care Ledger [care@ledger.fr](mailto:care@ledger.fr)

MM

Hi - I forwarded you the phishing email.. It was an email and it purportedly came from [support+recover@ledger.com](mailto:support+recover@ledger.com)  
I sent you the original email with headers as well as to the phishing email address at ledger and the support address at Onfido  
What is particularly concerning is that they have my information and are using it to create an attack vector.  
On Tue, Feb 25, 2025 at 10:03 PM Care Ledger <[care@ledger.fr](mailto:care@ledger.fr)> wrote:

## LEDGER SUPPORT

Hi,

Could you let me know the phone number or email of the people who contacted you please so that I can report this to the authorities?

Please continue to stay vigilant of all the possible scams in [this guide](#) and never share your [recovery phrase](#) with anyone.

Let me know if you have additional questions regarding this.

Kind regards,

Sybil  
Ledger Support

Visit the [Ledger Academy](#) to learn more about what Ledger does for you and your assets.

Our essentials - [Ledger Nano X](#), [Ledger Nano S+](#), [Ledger Backup Pack](#). Add an extra security layer to your assets with a [Cryptosteel](#), [Billfodl](#), or [Cryptotag Zeus](#).



This email was sent to you because you requested support at [support.Ledger.com](mailto:support.Ledger.com). We respect your right to privacy. Read our Privacy Policy and Cookie Policy. © Ledger SAS 2023. All rights reserved. Ledger brands are registered trademarks of Ledger SAS. Ledger SAS, 106 Rue du Temple, 75003 Paris, France.

thread::MX3iR-Mxcgm7AhDy8HSPbyi::

40. The next day, February 26, 2025, Mr. Mirashi received suspicious emails seeking his Apple credentials. He ignored these.

41. Mr. Mirashi also received two Google emails similar to the one he had received the day before. He ignored these as well.

42. At 3:47 p.m. Mr. Mirashi received an email from “Ledger Support” which informed him that the original phishing email was genuine and that he should follow the instructions, click on the link provided, and provide his extended public key.

**From:** Care Ledger  
mandarmirashi@gmail.com  
**Subject:** Re: Ledger Support - Case 00113667 [ thread::MX3iR-Mxcgm7AhDy8HSPbyl:: ]  
**Date:** February 26, 2025 at 3:47 PM  
**To:** Mandar Mirashi mandarmirashi@gmail.com



## LEDGER SUPPORT

Hi,

I checked over this email, and do conclude that this was not a phishing email. The email did in fact originate from our Ledger Recover Team.

This request is currently being processed, if you do not recognize it, we must proceed with you cancelling the recovery by providing your xPub key.

Please continue to stay vigilant of all the possible scams in [this guide](#) and never share your [recovery phrase](#) with anyone.

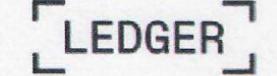
Let me know if you have additional questions regarding this.

Kind regards,

Sybil  
Ledger Support

Visit the [Ledger Academy](#) to learn more about what Ledger does for you and your assets.

Our essentials - [Ledger Nano X](#), [Ledger Nano S+](#), [Ledger Backup Pack](#). Add an extra security layer to your assets with a [Cryptosteel](#), [Billfodl](#), or [Cryptotag Zeus](#).



This email was sent to you because you requested support at [support.Ledger.com](#). We respect your right to privacy. Read our Privacy Policy and Cookie Policy. © Ledger SAS 2025. All rights reserved. Ledger brands are registered trademarks of Ledger SAS. Ledger SAS, 106 Rue du Temple, 75003 Paris, France.

thread::MX3iR-Mxcgm7AhDy8HSPbyl::

43. Mr. Mirashi responded at 6:45 p.m. that Ledger's conclusion did not make sense.

**From:** Mandar Mirashi mandarmirashi@gmail.com  
**Subject:** Re: Ledger Support - Case 00113667 [ thread::MX3iR-Mxcgm7AhDy8HSPbyl:: ]  
**Date:** February 26, 2025 at 6:45 PM  
**To:** Care Ledger care@ledger.fr



That does not make sense. I DO NOT have a ledger recover subscription.

Someone has fraudulently put in a subscription using my stolen identity information and is trying to hack me

MAndar  
845-380-7542

44. One minute later Mr. Mirashi received another “case closed” email.

45. At 7:24 p.m. Mr. Mirashi received another email from Care Ledger informing him that “after further review of this case” Ledger concluded that Mr. Mirashi was, in fact, enrolled in the Ledger Recover process, and that if he suspected any fraudulent activity he should complete the verification request and provide his extended public key to help Ledger protect him and his assets:

**From:** Care Ledger  
mandarmirashi@gmail.com  
**Subject:** Re: Ledger Support - Case 00113667 [ thread::MX3iR-Mxcgm7AhDy8HSPbyl:: ]  
**Date:** February 26, 2025 at 7:24 PM  
**To:** Mandar Mirashi mandarmirashi@gmail.com

## LEDGER SUPPORT

Hi,

After further review of this case, I can see that you are enrolled within the Ledger Recover process.

If you believe there is any fraudulent activity or the request itself is fraudulent, we urge you to complete the verification request as soon as you are able to. This will help aid us in protecting you and your assets.

You can generate your xPub [here](#), completely offline.

Please continue to stay vigilant of all the possible scams in [this guide](#) and never share your [recovery phrase](#) with anyone.

Let me know if you have additional questions regarding this.

Kind regards,

Sybil  
Ledger Support

Visit the [Ledger Academy](#) to learn more about what Ledger does for you and your assets.

Our essentials - [Ledger Nano X](#), [Ledger Nano S+](#), [Ledger Backup Pack](#). Add an extra security layer to your assets with a [Cryptosteel](#), [Billfodl](#), or [Cryptotag Zeus](#).

## LEDGER



This email was sent to you because you requested support at [support.Ledger.com](#). We respect your right to privacy. Read our Privacy Policy and Cookie Policy. © Ledger SAS 2023. All rights reserved. Ledger brands are registered trademarks of Ledger SAS. Ledger SAS, 106 Rue du Temple, 75003 Paris, France.

thread::MX3iR-Mxcgm7AhDy8HSPbyl::

46. Mr. Mirashi responded at 7:24 p.m. seeking further information, and a minute later received another “case closed” email.

47. At 7:41 p.m. Mr. Mirashi received an email from Care Ledger purporting to answer his questions.

**From:** Care Ledger  
mandarmirashi@gmail.com  
**Subject:** Re: Ledger Support - Case 00113667 [ thread::MX3iR-Mxcgm7AhDy8HSPbyl:: ]  
**Date:** February 26, 2025 at 7:41 PM  
**To:** Mandar Mirashi mandarmirashi@gmail.com

## LEDGER SUPPORT

Hi,

When Ledger Recover is enrolled, it is securely linked to your customer information and Ledger devices. The devices associated with your account are determined based on your purchase history, ensuring that only authorized devices are recognized.

Each device's serial ID is proprietary information recorded within our company's secure records, maintaining the confidentiality and integrity of your data.

Let me know if you have additional questions regarding this.

Kind regards,

Sybil  
Ledger Support

Visit the [Ledger Academy](#) to learn more about what Ledger does for you and your assets.

Our essentials - [Ledger Nano X](#), [Ledger Nano S+](#), [Ledger Backup Pack](#). Add an extra security layer to your assets with a [Cryptosteel](#), [Billfodl](#), or [Cryptotag Zeus](#).



This email was sent to you because you requested support at [support.Ledger.com](#). We respect your right to privacy. Read our Privacy Policy and Cookie Policy. © Ledger SAS 2023. All rights reserved. Ledger brands are registered trademarks of Ledger SAS. Ledger SAS, 106 Rue du Temple, 75003 Paris, France.

thread::MX3iR-Mxcgm7AhDy8HSPbyl::

48. Mr. Mirashi exchanged more emails with Care Ledger again at 8:11 and 8:21 p.m.

49. In the meantime, at 7:21 p.m. Mr. Mirashi posted in a Reddit group dedicated to Ledger issues and asked about the suspected phishing attempt requesting he provide his extended public key.

50. At 7:31 and 7:33 p.m. Reddit user “Large-Front-658” (since deleted) responded and encouraged Mr. Mirashi to respond to the Ledger email, complete the verification process, and provide his extended public key. But Mr. Mirashi did not do so (nor did he at any time).

The screenshot shows a Reddit thread in the **r/ledgerwallet** subreddit. The sidebar on the left includes links for Home, Popular, Answers (BETA), Explore, All, Create a custom feed, and RECENT. The main content area shows three deleted posts from users [deleted] and [deleted]. The first post discusses the official xpub tool and mentions running it offline through HTML. The second post asks if there's a way to check device IDs before attempting verification. The third post suggests disconnecting from the internet and using the tool offline on a computer. The sidebar on the right shows the subreddit stats: 161K users and 140 online.

51. Another Reddit user associated with Ledger itself later responded to Mr. Mirashi warning him not to respond to the email, saying it was a scam.

52. A few minutes after this warning response, at 8:30 p.m., Mr. Mirashi found that his Reddit account of 16 years had been deleted.

53. Mr. Mirashi immediately suspected that his system had been severely compromised since someone would need his Reddit password to delete his account.

54. At 8:34 p.m., a few minutes after his Reddit account was deleted, Mr. Mirashi moved 300 BTC from his Ledger wallet to his Electrum hot wallet because he believed his Ledger wallet might be compromised.

55. He also immediately changed his Google password, and began the laborious process of changing his other passwords.

56. At no point did Mr. Mirashi provide his private key to anyone, nor was it stored on his computer.

### The Attempted Theft Of Mr. Mirashi's BTC

57. Suddenly at 9:14 p.m. Mr. Mirashi saw a pending transaction attempting to move 302 BTC from his Electrum wallet to address bc1q8fvx5trkyfvt9xmj43pmum9de76lhq0euntngr (referred to as the “Hacker address”) which was not an address Mr. Mirashi knew.

Advanced Details			
Hash	bd63-07ac	Time	26 Feb 2025 09:14:39
Age	8d 21h 13m 5s	Inputs	6
Input Value	302.00540087 BTC	Outputs	1
	\$26,090,681	Output Value	302.00535092 BTC
Fee	0.00004995 BTC		\$26,090,677
	\$4.32	Fee/B	5.365 sat/B
Fee/VB	11,150 sat/vByte	Size	931 Bytes
Weight	1,792	Weight Unit	2.787 sat/WU
Coinbase	No	Witness	Yes
RBF	Yes	Locktime	885,489
Version	2	BTC Price	\$86,391.44

58. Mr. Mirashi acted immediately and successfully nullified the transaction before it was confirmed on the bitcoin blockchain, as shown by the red “Invalid” transaction record above.

59. Mr. Mirashi then immediately moved the BTC back to the Ledger wallet.

60. Mr. Mirashi believed he had avoided disaster because he had changed all the passwords.

## The Theft Of The BTC

61. However, the following afternoon at 2:20 p.m. on February 27, 2025, 521.99931468 BTC was stolen from Mr. Mirashi's two Ledger wallets and sent to the Hacker's address:

TX		USD	Summary			
<b>Bitcoin Transaction</b>						
Broadcasted on 27 Feb 2025 02:20:10 GMT-5						
Hash ID 1c4e05899d0a0d89df654b91eed7d6e5ce28f636 09734264836410cd833dc19						
<b>Amount</b>	521.99931468 BTC + \$45,151,385	USD	<b>Block ID</b>	885,606		
<b>Fee</b>	89,600 SATS + \$77.50		<b>Time</b>	27 Feb 2025 02:20:10		
<b>From</b>	2 Inputs		<b>Inputs</b>	2		
<b>To</b>	bc1q8-ntngr		<b>Outputs</b>	1		
<b>Confirmed</b>						
 This transaction has 1,185 Confirmations. It was mined in Block 885,606						
 This transaction paid ~40% more in fees due to inefficiencies associated with older wallets.						
<a href="#">Learn More</a>						
<a href="#">Overview</a> <a href="#">JSON</a>						
<b>From</b>						
 1 36cfw3QeJryX7JbWb1DKL7ZP1zMuF15 219.99510525 BTC + \$19,028,921						
 2 33oV5phndHe1PfUqj1NH9fVUzNhAeDLHAN 302.00510543 BTC + \$26,122,541						
<b>To</b>						
 1 bc1q8fvx5trkyfvt9xmj43pmr9de76lhq0euntrng 521.99931468 BTC + \$45,151,385						

62. Mr. Mirashi discovered the theft at around 5 p.m. He immediately contacted Ledger support and the FBI.

## Tracking The Bitcoin After The Theft

63. One of the features of blockchain technology is transparency. A record of the movement and transfers of various assets can be reviewed on the bitcoin blockchain. Each transaction has a unique identifier.

64. Another feature of blockchain technology is its relative anonymity. Blockchain users are identified by their public wallet addresses, not their names.

65. As is typical in cryptocurrency thefts, John Doe has moved the Stolen Assets many times to try to obscure the trail.

66. Mr. Mirashi retained Token Recovery, a blockchain analysis company, to track the Stolen Assets.

67. From the Hacker address, Mr. Mirashi's BTC was split up and moved around to 197 private wallet addresses and 140 addresses associated with virtual asset service providers (VASPs) in 668 transactions.

68. Plaintiff has identified five VASPs and one unidentified exchange or exchanges that received deposits of Mr. Mirashi's BTC, which are named as Relief Defendants.

69. As of this date 353 BTC have been deposited with the Relief Defendants.

70. Relief Defendant FixedFloat received 70 deposits.

71. Relief Defendant ChangeNow received 4 deposits.

72. Relief Defendant Kraken received 38 deposits.

73. Relief Defendant eXch.cx received 15 deposits.

74. Relief Defendant TradeOgre received 70 deposits.

75. Relief Defendant John Doe has received 45 deposits.

76. In addition, 169.24 of Mr. Mirashi's BTC has been located in five private wallets on the bitcoin blockchain. These wallet addresses are:

bc1qedyy7dfqz7kcesk8ap5kv0sq90c0cctv75fjda;

bc1q5uhs4kwaq685hx2p9klhzufw6kzck65x9znuva;

bc1qwjtuqew73j8zhc0xhezx905fvytj5g4307czjf;

35sBUp4t5t8gerEu9HswPiNhRSTnnS8qWX; and

38WP9sta67jMzwPrzWfrGMci7qVCpX4cFY.

## CAUSES OF ACTION

### COUNT ONE

#### **Violation Of The Computer Fraud And Abuse Act ("CFAA") 18 U.S.C. §1030 *et seq.***

77. Plaintiff repeats and realleges the above paragraphs as if fully set forth herein.

78. The CFAA gives Plaintiff a private right of action against computer hackers.

79. Plaintiff's computer is equipped with email, internet browsing software, and access to social media. Accordingly, Plaintiff's computer is a "protected" computer used in interstate commerce and communication.

80. John Doe had no authorization to access Plaintiff's computer.

81. John Doe knowingly accessed Plaintiff's computer did so with the intent to defraud and steal from Plaintiff.

82. John Doe used the unauthorized access to steal 521.99931468 BTC from Plaintiff, far exceeding the CFAA minimum threshold of \$5,000.

83. Plaintiff is entitled to compensatory damages.

84. Plaintiff is further entitled to injunctive and equitable relief pursuant to the CFAA including but not limited to (i) an order enjoining John Doe from accessing plaintiffs wallets; (ii) an order requiring John Doe to disgorge his ill-gotten gains; (iii) an order for an accounting of the amount and location of Plaintiff's Stolen Assets; (iv) an order imposing a constructive trust; (v) an order freezing the assets of John Doe; and (vi) an order enjoining the further transfer or disposition of Plaintiff's stolen assets by any party.

**COUNT TWO**

**Violation of New Jersey Computer-Related Offenses Act, N.J.S.A. § 2A:38A**

85. Plaintiff repeats and realleges the above paragraphs as if fully set forth herein.

86. Defendant John Doe purposefully, knowingly and without authorization, took data from Plaintiff's computer, *i.e.* the passcodes to Plaintiff's software wallets, in violation of N.J.S.A. §2A:38A-3(a).

87. Plaintiff is entitled to compensatory damages, punitive damages, costs of suit, attorneys fees, costs of investigation, and litigation costs pursuant to N.J.S.A. §2A:38A-3.

88. Plaintiff is further entitled to injunctive and equitable relief pursuant to N.J.S.A. §2A:38A-5, including but not limited to (i) an order enjoining John Doe from accessing plaintiffs wallets; (ii) an order requiring John Doe to disgorge his ill-gotten gains; (iii) an order for an accounting of the amount and location of Plaintiff's stolen assets; (iv) an order imposing a constructive trust; (v) an order freezing the assets of John Doe; and (vi) an order enjoining the further transfer or disposition of Plaintiff's stolen assets by any party.

**COUNT THREE**

**Common Law Fraud**

89. Plaintiff repeats and realleges the above paragraphs as if fully set forth herein.

90. On February 26 and 27, 2025 John Doe sent various phishing emails to Plaintiff impersonating Google and/or Ledger.

91. As a result of these phishing emails, John Doe was able steal Plaintiff's BTC.

92. Plaintiff is entitled to actual, compensatory, and punitive damages.

**COUNT FOUR**

**Conversion**

93. Plaintiff repeats and realleges the above paragraphs as if fully set forth herein.

94. As of February 27, 2025, Plaintiff owned and had the right to possess the Stolen Assets.

95. When John Doe drained Plaintiff's crypto wallets of BTC, John Doe intentionally took possession of, and assumed control over, the Stolen Assets.

96. John Doe has intentionally exercised control, and continues to exercise control, over the Stolen Assets in such a way as to preclude Plaintiff from using or possessing the Stolen Assets.

97. John Doe knew the Stolen Assets were stolen or obtained in a manner constituting theft.

98. Accordingly, John Doe wrongfully converted the Stolen Assets.

99. As a direct and proximate result of the conversion, Plaintiff suffered damages and continues to suffer damages as long as the Stolen Assets are in the possession of John Doe.

100. Plaintiff is entitled to actual damages, compensatory damages, interest, expenses, and any other relief the court deems just and proper.

**COUNT FIVE**  
**Replevin under N.J.S.A 2B:50-1**

101. Plaintiff repeats and realleges the above paragraphs as if fully set forth herein.

102. On February 27, 2025, John Doe acquired possession of the Stolen Assets from Plaintiff through fraud, and John Doe wrongly holds the Stolen Assets.

103. John Doe has intentionally exercised control, and continues to exercise control, over the Stolen Assets in such a way as to preclude Plaintiff from using or possessing the Stolen Assets.

104. John Doe has no right to possess the Stolen Assets.

105. John Doe did not take the Stolen Assets to satisfy any tax, assessment, lien, or attachment against Plaintiff.

106. Plaintiff is entitled to the return of the Stolen Assets and other relief that the court may deem just and proper.

**COUNT SIX**  
**Unjust Enrichment**

107. Plaintiff repeats and realleges the above paragraphs as if fully set forth herein.

108. John Doe obtained a benefit when he stole Plaintiff's BTC.

109. Under the circumstances, it would be against equity and good conscience to permit John Doe to retain the Stolen Assets.

110. Plaintiff is entitled to restitution and such other relief as the court deems just and proper.

**COUNT SEVEN**

**Equitable Relief Against John Doe and the Relief Defendants:**

**(i) Enjoining Current and Future Holders Of The Stolen Assets From Transferring Or Disposing Of The Stolen Assets; (ii) Enjoining Current and Future Holders Of The Stolen Assets To Disgorge the Stolen Assets; (iii) Establishing a Constructive Trust Over the Stolen Assets; and (iv) An Accounting of the Stolen Assets.**

111. Plaintiff repeats and realleges the above paragraphs as if fully set forth herein.

112. Plaintiff and his expert have traced the Stolen Assets to certain wallets whose owners are unknown and to certain identifiable VASPs.

113. The assets stolen by John Doe are specific and identifiable property and can be traced to John Doe.

114. In order to further prevent the dissipation of the Stolen Assets, Plaintiff requests an order enjoining the transfer or disposition of those assets, including present and future holders of the Stolen Assets.

115. The Stolen Assets being held by John Doe and the Relief Defendants must be disgorged to Plaintiff because John Doe is not entitled to the benefits of the Stolen Assets.

116. The Stolen Assets must be held in trust for Plaintiff because John Doe is not entitled to the benefits of the Stolen Assets.

117. John Doe has attempted to dissipate the Stolen Assets with the goal of making the Stolen Assets difficult to track.

118. Plaintiff requests an accounting as to the location of the Stolen Assets.

119. Plaintiff requests the imposition of a constructive trust upon the property that was stolen from him by John Doe.

**PRAYER FOR RELIEF**

WHEREFORE, Plaintiff demands judgment in his favor and against defendant John Doe as follows:

- a. An injunction ordering John Doe and the Relief Defendants to disgorge the Stolen Assets;
- b. An injunction preventing any unknown holders of John Doe's Stolen Assets from transferring or otherwise disposing of the Stolen Assets.
- c. An injunction ordering any unknown holders of John Doe's Stolen Assets to disgorge the Stolen Assets.
- d. An order awarding Plaintiff actual, compensatory and consequential damages;
- e. An order awarding Plaintiff punitive damages in an amount to be determined but no less than \$1 million.
- f. An order awarding Plaintiff pre- and post- judgment interest;
- g. An order awarding Plaintiff attorney's fees, expert and consultant fees and expenses, and costs; and
- h. Such other and further legal and equitable relief as the court deems just and proper.

**DEMAND FOR JURY TRIAL**

Plaintiff demands a jury trial for all issues so triable.

Dated: March 11, 2025

Law Office of Adam R. Gonnelli, L.L.C.

By   
Adam Gonnelli

707 Alexander Road  
Building 2, Suite 208  
Princeton, New Jersey 08540  
phone: (917) 541-7110  
[adam@arglawoffice.com](mailto:adam@arglawoffice.com)

Attorneys for Plaintiff