UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF FLORIDA

Civil Action No. _____

TULLIA HEISSENBERG, an individual,

Plaintiff,

v.

JOHN DOE, an individual;

Defendant.

_____/

COMPLAINT FOR DAMAGES AND EQUITABLE RELIEF

Plaintiff TULLIA HEISSENBERG, an individual (hereafter referred to as "Plaintiff"), by and through undersigned counsel, hereby sues Defendant JOHN DOE, an individual; for damages and equitable relief. As grounds therefor, Plaintiff alleges the following:

PRELIMINARY STATEMENT

1. This action is brought by Plaintiff, a retired senior citizen who lost approximately Four Million Four Hundred Thousand Dollars ($4,400,000.00) worth of cryptocurrency in an ongoing identity theft crime called "SIM swapping" or "SIM hijacking."

2. "SIM swapping" is not merely an ongoing crime; it is a booming crime -- especially one that targets cryptocurrency investors.

3. Over the past three years alone, undersigned counsel has represented nearly one hundred (100) SIM swapping victims across the country whose individual cryptocurrency losses have ranged from as little as $3,000.00 to as much as $12,500,000.00.

4. Of those 100-or-so cases, few if any represent stories as egregious as the targeted crime committed upon Plaintiff; as she was SIM swapped not once, not twice, not three times, not four

times, but five times over a six-month period before the criminal actors succeeded in stealing her cryptocurrency assets.

5. JOHN DOE -- with vital assistance from at least one insider at the telecommunications provider (Metro by T-Mobile) through whom Plaintiff received her monthly cellphone service -- played a material role in the scheme to steal Plaintiff's assets and, upon information and belief, currently possesses all or a significant portion of Plaintiff's stolen property.

6. Plaintiff brings this lawsuit to recover her stolen assets.

PARTIES, JURISDICTION AND VENUE

THE PARTIES

Plaintiff

7. Plaintiff TULLIA HEISSENBERG is an individual domiciled in Delray Beach, Florida, is a citizen of the state of Florida, and is *sui juris*.

Defendant

8. Defendant JOHN DOE is an individual and, upon information and belief, is *sui juris*.

9. At all times material hereto, JOHN DOE has maintained -- and continues to maintain as of the date of this filing -- private cryptocurrency wallets and cryptocurrency exchange accounts in which JOHN DOE holds all or a portion of the cryptocurrency stolen from Plaintiff.

Other Liable Persons/Entities

10. Plaintiff is prosecuting against Metro by T-Mobile in the private arbitration forum required by Metro by T-Mobile's Terms and Conditions of Service (American Arbitration Association) her claims for the liability Metro by T-Mobile bears for its insiders' acts and omissions in connection with the appalling harm inflicted upon Plaintiff. Should Metro by T-Mobile agree to waive its insistence that Plaintiff's claim be hidden from public scrutiny -- or should the arbitrator presiding over that proceeding declare unconscionable or void as against public policy Metro by T-Mobile's

Terms and Conditions of Service (including its requirement that claims such as Plaintiff's be arbitrated) -- Plaintiff will join Metro by T-Mobile as a defendant in the instant matter.

11. In addition to Defendant and Metro by T-Mobile, there are likely other parties who may be liable to Plaintiff, but about whom Plaintiff currently lacks specific facts to permit her to name these persons or entities as party defendants. By not naming such persons or entities at this time, Plaintiff is not waiving her right to amend this pleading to add such parties, should the facts warrant adding such parties.

JURISDICTION AND VENUE

12. This Court has subject matter jurisdiction over this action pursuant to 28 U.S.C. § 1332 because the amount in controversy exceeds Seventy-Five Thousand Dollars ($75,000.00), exclusive of interest, costs and attorneys' fees, and is an action between citizens of different states.

13. This Court also has subject matter jurisdiction over this action 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(a), *et seq.*).

14. This Court has personal jurisdiction over Defendant because he committed a tort in this jurisdiction.

15. Venue of this action is proper in this Court pursuant to 28 U.S.C. § 1391 because the causes of action accrued in this jurisdiction.

GENERAL FACTUAL ALLEGATIONS

How SIM Swapping Works

16. "SIM swapping," or "SIM hijacking" is a growing crime in the telecommunications world that requires little more than a thorough Google search, a willing telecommunications carrier representative, and an electronic or in-person impersonation of the victim.

17. To activate a mobile device for use on cellular telephone networks, many devices were assigned a unique International Mobile Equipment Identity ("IMEI") number in combination with a unique Subscriber Identity Module ("SIM"), enclosed on a small removable chip or directly embedded into the mobile device. This IMEI/SIM combination -- when paired with a customer's mobile telephone number assigned by a telecommunications carrier -- allows a given user to authenticate on a mobile phone carrier's network to make and receive cellular calls and text messages associated with the customer's mobile telephone number.

18. Generally, "SIM swapping" refers to a method of unauthorized takeover of a victim's wireless account by malicious actors such as JOHN DOE, carried out by linking the victim's mobile telephone number to a SIM card installed in a device controlled by the attacker(s). A typical SIM swap is illustrated below:

19. SIM swaps are commonly executed by attackers who gain unauthorized access to a wireless provider's computer networks or who gain such access with the assistance of witting or unwitting individuals who had access to the telecommunications provider's networks.

20. Often working in tandem with a telecommunications provider's employees -- who sometimes purposefully leak consumer data to third parties and/or the internet as a whole -- an unauthorized person contacts the telecommunications provider's technical support department on the phone, or walks into a telecommunications provider's retail store, intent on assuming the electronic identity of the target of the crime by possessing and utilizing information that only the telecommunications provider should have.

21. By getting the target's wireless telephone number transferred to a new SIM card that he owns, the thief works with the telecommunications provider to utilize the information provided to him by the telecommunications provider and/or to simply **bypass all security measures** in place on the accountholder's account to effectuate the transfer.

22. Whether acting as a co-conspirator to the theft or through willful and/or abject negligence, the telecommunications provider transfers (or "ports") to the unauthorized person the accountholder's wireless telephone number -- disconnecting the telephone number from the actual accountholder's wireless phone's SIM card and then connecting the telephone number to a SIM card under the control of the unauthorized person.

23. As discussed above, in some cases, upon information and belief, telecommunications provider employees also provide the thief sacrosanct personal information about the targeted accountholder, including his/her security PIN code(s) and his electronic mail address. That information is critical to effectuating the SIM swap.

24. From there, the victim loses cellphone service (including the ability to send or receive talk, text, or data transmissions), given that only one SIM card can be connected to the telecommunications provider's network with any given telephone number at a time.

25. As a result of the SIM swap, phone calls and SMS text messages sent to the victim's mobile telephone number are routed to a device controlled by the attacker(s), giving the attacker(s) complete control over the victim's mobile telephone number.

26. Using the information provided by the telecommunications provider insider(s), the thief then assumes the victim's electronic identity, beginning with his/her electronic mail address, which the thief overtakes employing a simple "Password Reset" feature that requires control of the victim's cellphone number (which was supplied to the thief by the telecommunications provider insider[s]).

27. Having been delivered the victim's cellular telephone number and, directly or indirectly, his/her electronic mail address, the thief then diverts to himself access to the victim's banking and investment accounts (including cryptocurrency holdings) by similarly using the victim's cellular telephone number as a "recovery method" to reset passwords and access to those accounts -- even if the victim had two-factor authentication activated as a security measure on his/her accounts.

28. At that point, the thief absconds with the victim's cryptocurrency holdings and other personal assets.

29. To be clear, simply *knowing* an accountholder's cellphone number or e-mail address is not enough. The key is having **control** over and securing those vital electronic gateways to information and communication; and telecommunications providers regularly and contumaciously place the keys to those gates directly into the hands of unauthorized persons like JOHN DOE while simultaneously denying their accountholders their power over such things.

The Anatomy of Plaintiff's SIM Swaps

30. In the instant matter, insiders at Metro by T-Mobile -- whether acting as a co-conspirators to the theft or through abject negligence -- transferred to JOHN DOE control over Plaintiff's mobile telephone number and e-mail address, which **on its fifth SIM swap** ultimately led to the theft of approximately Four Million Four Hundred Thousand Dollars ($4,400,000.00) in cryptocurrency assets from Plaintiff on or about March 1, 2021.

a. The First SIM Swap

31. At or about 11:52 p.m. EST on **October 25, 2020**, a Metro by T-Mobile representative(s) bypassed Metro by T-Mobile's security protocols and transferred to an unauthorized person Plaintiff's wireless telephone number -- disconnecting the telephone number from Plaintiff's wireless phone's SIM card and then connecting the telephone number to a SIM card under the control of the unauthorized person.

32. Plaintiff went to a T-Mobile corporate store near her home to explain her problem and express her frustration with the unauthorized transfer of her cellular phone service.

33. At Plaintiff's insistence, Metro by T-Mobile changed the SIM card number back to Plaintiff's cellphone, restoring her phone service.

34. Metro by T-Mobile also assured Plaintiff at that time that additional security measures would be implemented on Plaintiff's Metro by T-Mobile account to prevent future unauthorized activity or SIM card swapping. Among the changes made were implementation of a longer PIN on Plaintiff's Metro by T-Mobile account and Metro by T-Mobile's explicit assurance to Plaintiff that no changes could be made over the telephone. Plaintiff was told by Metro by T-Mobile that she would be afforded the highest level of security on her account and that no future SIM transfers would be allowed unless the request were made in a Metro by T-Mobile store and the person making the request were fully vetted with proper identification.

35. Those promises of safety and security rang entirely hollow, as the SIM swaps targeting Plaintiff were just getting started.

b. The Second SIM Swap

36. At or about 1:58 p.m. EST on **January 31, 2021**, a Metro by T-Mobile representative(s) again bypassed Metro by T-Mobile's security protocols and transferred to an unauthorized person Plaintiff's wireless telephone number -- disconnecting the telephone number from Plaintiff's wireless phone's SIM card and then connecting the telephone number to a SIM card under the control of the unauthorized person.

37. Plaintiff again went to a T-Mobile corporate store near her home to again express her frustration with the unauthorized transfer of her cellular phone service that violated all of the advanced security protocols that had been promised to her by Metro by T-Mobile.

38. At Plaintiff's insistence, Metro by T-Mobile again changed the SIM card number back to Plaintiff's cellphone, restoring her phone service.

39. Plaintiff also changed the security code on her Metro by T-Mobile account to a new secure code, described to her by the Metro by T-Mobile representative at that time as a "high security key."

c. The Third SIM Swap

40. At or about 2:26 a.m. EST on **February 5, 2021**, a Metro by T-Mobile representative(s) again bypassed Metro by T-Mobile's security protocols and transferred to an unauthorized person Plaintiff's wireless telephone number -- disconnecting the telephone number from Plaintiff's wireless phone's SIM card and then connecting the telephone number to a SIM card under the control of the unauthorized person.

41. No Metro by T-Mobile retail store was open at that hour, so the SIM transfer obviously could not have been authorized in-person with properly verified identification -- as required by the enhanced security protocols implemented by Metro by T-Mobile on Plaintiff's account.

42. Once more, Plaintiff went to a T-Mobile corporate store near her home to remedy the situation; and once more, at Plaintiff's insistence, Metro by T-Mobile changed the SIM card number back to Plaintiff's cellphone, restoring her phone service.

43. Plaintiff again changed the security code on her Metro by T-Mobile account to a new secure code and was assured by a Metro by T-Mobile representative that Plaintiff was "totally safe."

d. The Fourth and Fifth SIM Swaps

44. At or about 4:49 a.m. EST on **February 26, 2021** and at about 12:50 a.m. EST on **February 28, 2021**, Metro by T-Mobile representatives again bypassed Metro by T-Mobile's security protocols and transferred to an unauthorized person Plaintiff's wireless telephone number -- disconnecting the telephone number from Plaintiff's wireless phone's SIM card and then connecting the telephone number to a SIM card under the control of the unauthorized person.

45. No Metro by T-Mobile retail store was open at those hours, so the SIM transfer obviously could not have been authorized in-person with properly verified identification -- as required by the enhanced security protocols implemented by Metro by T-Mobile on Plaintiff's account.

46. At the time of the fourth and fifth SIM swaps, Plaintiff was traveling outside the United States; and she did not return to her home in Florida until March 8, 2021.

47. Unfortunately, before she returned home, Plaintiff was robbed by JOHN DOE.

John Doe's Theft of Plaintiff's Cryptocurrency Holdings

48. While controlling Plaintiff's cellphone number, JOHN DOE was able to access Plaintiff's account at cryptocurrency exchange BlockFi, where Plaintiff stored a valuable cryptocurrency portfolio.

49. Commencing on or about March 1, 2021 at 20:01 UTC, JOHN DOE withdrew from Plaintiff's BlockFi account the following cryptocurrency assets -- all without Plaintiff's knowledge or authorization -- and deposited those stolen assets into two cryptocurrency wallets owned or controlled by or for JOHN DOE: bc1qdjkc4e3u8jup6axtda560z720vapq5p34pmwgu (the "JOHN DOE BTC Wallet") and 0xC51f0cbf92030F50829B244f8D876d5843b8A955 (the "JOHN DOE ETH Wallet") (collectively, the "JOHN DOE Wallet Addresses"), *to wit*:

#	Transfer Date (UTC)	Asset sent to JOHN DOE Wallet Address or Fee Charged	JOHN DOE Wallet Address
1	2021-03-01 20:01:47Z	4.9975 BTC	bc1qdjkc4e3u8jup6axtda560z 720vapq5p34pmwgu
2	2021-03-01 20:01:47Z	0.0025 BTC Withdrawal Fee	
3	2021-03-01 20:01:52Z	99.9985 ETH	0xC51f0cbf92030F50829B244 f8D876d5843b8A955
4	2021-03-01 20:01:52Z	0.0015 ETH Withdrawal Fee	
5	2021-03-01 20:01:54Z	99.9985 ETH	0xC51f0cbf92030F50829B244 f8D876d5843b8A955
6	2021-03-01 20:01:54Z	0.0015 ETH Withdrawal Fee	
7	2021-03-01 20:01:56Z	99.9985 ETH	0xC51f0cbf92030F50829B244 f8D876d5843b8A955
8	2021-03-01 20:01:56Z	0.0015 ETH Withdrawal Fee	
9	2021-03-01 20:01:59Z	99.9985 ETH	0xC51f0cbf92030F50829B244 f8D876d5843b8A955
10	2021-03-01 20:01:59Z	0.0015 ETH Withdrawal Fee	
11	2021-03-01 20:02:01Z	99.9985 ETH	0xC51f0cbf92030F50829B244 f8D876d5843b8A955
12	2021-03-01 20:02:01Z	0.0015 ETH Withdrawal Fee	

13	2021-03-01 20:02:04Z	99.9985 ETH	0xC51f0cbf92030F50829B244 f8D876d5843b8A955
14	2021-03-01 20:02:04Z	0.0015 ETH Withdrawal Fee	
15	2021-03-01 20:02:16Z	99.9985 ETH	0xC51f0cbf92030F50829B244 f8D876d5843b8A955
16	2021-03-01 20:02:16Z	0.0015 ETH Withdrawal Fee	
17	2021-03-01 20:02:18Z	99.9985 ETH	0xC51f0cbf92030F50829B244 f8D876d5843b8A955
18	2021-03-01 20:02:18Z	0.0015 ETH Withdrawal Fee	
19	2021-03-01 20:02:45Z	4.9975 BTC	bc1qdjkc4e3u8jup6axtda560z 720vapq5p34pmwgu
20	2021-03-01 20:02:45Z	0.0025 BTC Withdrawal Fee	
21	2021-03-01 20:03:06Z	4.9975 BTC	bc1qdjkc4e3u8jup6axtda560z 720vapq5p34pmwgu
22	2021-03-01 20:03:06Z	0.0025 BTC Withdrawal Fee	
23	2021-03-01 20:03:32Z	49.9985 ETH	0xC51f0cbf92030F50829B244 f8D876d5843b8A955
24	2021-03-01 20:03:32Z	0.0015 ETH Withdrawal Fee	
25	2021-03-01 20:03:39Z	49.9985 ETH	0xC51f0cbf92030F50829B244 f8D876d5843b8A955
26	2021-03-01 20:03:39Z	0.0015 ETH Withdrawal Fee	
27	2021-03-01 20:03:43Z	49.9985 ETH	0xC51f0cbf92030F50829B244 f8D876d5843b8A955
28	2021-03-01 20:03:43Z	0.0015 ETH Withdrawal Fee	
29	2021-03-01 20:03:45Z	49.9985 ETH	0xC51f0cbf92030F50829B244 f8D876d5843b8A955
30	2021-03-01 20:03:45Z	0.0015 ETH Withdrawal Fee	
31	2021-03-01 20:03:47Z	49.9985 ETH	0xC51f0cbf92030F50829B244 f8D876d5843b8A955

SILVER MILLER
11780 West Sample Road • Coral Springs, Florida 33065 • Telephone (954) 516-6000
www.SilverMillerLaw.com

32	2021-03-01 20:03:47Z	0.0015 ETH Withdrawal Fee	
33	2021-03-01 20:03:49Z	49.9985 ETH	0xC51f0cbf92030F50829B244 f8D876d5843b8A955
34	2021-03-01 20:03:49Z	0.0015 ETH Withdrawal Fee	
35	2021-03-01 20:04:16Z	5 BTC	bc1qdjkc4e3u8jup6axtda560z 720vapq5p34pmwgu
36	2021-03-01 20:05:08Z	4.9975 BTC	bc1qdjkc4e3u8jup6axtda560z 720vapq5p34pmwgu
37	2021-03-01 20:05:08Z	0.0025 BTC Withdrawal Fee	
38	2021-03-01 20:40:19Z	2.9975 BTC	bc1qdjkc4e3u8jup6axtda560z 720vapq5p34pmwgu
39	2021-03-01 20:40:19Z	0.0025 BTC Withdrawal Fee	
40	2021-03-03 21:53:20Z	0.024 BTC	bc1qdjkc4e3u8jup6axtda560z 720vapq5p34pmwgu
41	2021-03-03 21:53:20Z	0.0025 BTC Withdrawal Fee	
42	2021-03-03 22:54:50Z	8 ETH	0xC51f0cbf92030F50829B244 f8D876d5843b8A955

TOTALS	**28.0265 BTC**
	1108 ETH

50. As shown above, with almost every unauthorized withdrawal by JOHN DOE, Plaintiff's BlockFi account was assessed a withdrawal fee that further diminished Plaintiff's cryptocurrency holdings. In essence, the cryptocurrencies from Plaintiff's BlockFi holdings that were used to pay the withdrawal fees were likewise stolen from Plaintiff, as they were forcibly taken from her without her knowledge or authorization.

51. From the JOHN DOE Wallet Addresses, many of the stolen assets were then transferred to other wallets/accounts maintained by or for JOHN DOE (collectively, the "JOHN DOE Secondary Addresses"), *to wit*:

#	Recipient Cryptocurrency Exchange	Destination Address	Asset and Tracing Amount
1		bc1qfwxkmzln5g3g0n8vw5dqsv4vtxumh5xscyzr9l	4.777099848 BTC
2		bc1qkjhlymppxz4g4h6xle8u6scd8d6tm8s657zqqy	3.401842272 BTC
3	Xapo.com	19JyAkHKh36sFduqK4hMsMZhU6ZDoLotW	2.33906575 BTC
4		13jWBgfYQRs1pPwsWhk9jtvjfDMgdByknP	2.20246077 BTC
5		bc1qe8esnkcwyvnnfe5f3ksfmj9eyktq9u0635lhuv	1.478941262 BTC
6		327uTRES6ThXupKUAt1Xuk2pD9BiZaZ4wT	1.10657357 BTC
7	BitPay	15oRB2myPpq8h1jTdRDKE58WXPpSYgK6Qr	1.105248136 BTC
8	Poloniex	12vZ3fU66g4XTeomUYCEPp9rcsWjexgzR7	0.497294128 BTC
9	Binance	15cxBdcNYsdkTW6JoM3Q4xshRF6x8vYrEc	0.41288896 BTC
10	Coinbase	3LF1XGESznTATC7dMQ2zWmZdf4WEJCcehj	0.3 BTC
11	Gemini	bc1qss5ejcqfrmjm9lfydshanhjkc7wnlhk4khlsj8	0.250298812 BTC
12	Binance	e86433d2068bd319a54128117849b511f3e0ed42	1091.1566815047 ETH
13	Coincheck	24ba1542f8a0a20e8251d096213384cfb0ee3dbc	6.322870267 ETH
14		0c32245e86764a61de9feaad1315ac7ceaac70b2	0.0135378573 ETH
15		85dbca0a9bfee831f266065b6142f9ed3b5b1dd7	7.9214341878 ETH
16		a1b78d4c51c50f30c936c3f941c2e206b71b3983	0.0005026098 ETH
17		f7dddfbdb3ea8e0cadf101f37fe08695a955e25c	0.0180210793 ETH
18	Binance	bfaa724c8fc49e490947e4c7c8d597b6336b67ac	0.621182859 ETH
19		2fbbfe6e64d55168cf1ccfc993e61f2c4aa1ef06	0.0239687943 ETH
20		9b5b25216601f065aacbe8e641fa897163a69c2b	1.6162668327 ETH
21		6da237bb6942e5d807a5ac55e7d17e487688d5ee	0.0329650529 ETH
22		31385d3520bced94f77aae104b406994d8f2168c	0.0100385744 ETH

TOTALS	**17.87171351 BTC**
	1107.73746962 ETH

52. As of the date of this filing, the 28.0265 BTC and 1108 ETH stolen from Plaintiff are valued at approximately Four Million Four Hundred Thousand Dollars ($4,400,000.00).

53. As a result of the actions described above, Plaintiff has suffered damages in an amount that will be proven at trial.

54. Plaintiff duly performed all of her duties and obligations; and any conditions precedent to Plaintiff bringing this action have occurred, have been performed, or else have been excused or waived.

55. To enforce her rights, Plaintiff has retained undersigned counsel and is obligated to pay counsel a reasonable fee for its services.

COUNT I – CONVERSION

Plaintiff re-alleges, and adopts by reference herein, Paragraphs 1 - 55 above, and further alleges:

56. On March 1, 2021, at the time of the hack, Plaintiff owned and had the right to immediately possess the 28.0265 BTC and 1108 ETH -- not just a mere right to payment for the value of those cryptocurrencies -- that were taken from her and transferred to the JOHN DOE Wallet Addresses and/or the JOHN DOE Secondary Addresses.

57. When the stolen bitcoin was deposited by a thief/thieves into the JOHN DOE Wallet Addresses and later moved to the JOHN DOE Secondary Addresses, JOHN DOE intentionally took possession of and assumed control over the 28.0265 BTC and 1108 ETH.

58. JOHN DOE has intentionally exercised control, and continues to exercise control, over the bitcoin in such a way as to exclude Plaintiff from using or possessing the 28.0265 BTC and 1108 ETH.

59. JOHN DOE knew the property he received was stolen or obtained in a manner constituting theft.

60. As such, JOHN DOE wrongfully converted the 28.0265 BTC and 1108 ETH.

61. As a direct and proximate result of the foregoing, Plaintiff suffered the wrongful conversion of personal property whose value exceeds Seventy-Five Thousand Dollars ($75,000.00).

WHEREFORE, Plaintiff TULLIA HEISSENBERG, an individual, demands entry of a judgment against Defendant JOHN DOE, an individual; for damages, including compensatory damages, interest, expenses, and any other relief the Court deems just and proper.

COUNT II – REPLEVIN

Plaintiff re-alleges, and adopts by reference herein, Paragraphs 1 - 55 above, and further alleges:

62. This is an action to recover possession of personal property.

63. The property at issue is 28.0265 BTC and 1108 ETH.

64. Upon information and belief, the U.S. Dollar equivalent value of the personal property as of the date of theft is approximately Four Million Four Hundred Thousand Dollars ($4,400,000.00).

65. As of the date of this filing, the personal property is believed to be stored in the JOHN DOE Wallet Addresses and/or the JOHN DOE Secondary Addresses delineated above.

66. On March 1, 2021, at the time of the hack, Plaintiff owned and had the right to immediately possess the personal property -- not just a mere right to payment for the value of those cryptocurrencies -- that was taken from her.

67. JOHN DOE has intentionally exercised control, and continues to exercise control, over the cryptocurrencies in such a way as to exclude Plaintiff from using or possessing them.

68. The property has not been taken for any tax, assessment or fine pursuant to law, nor has it been taken under an execution or attachment against Plaintiff's property.

WHEREFORE, Plaintiff TULLIA HEISSENBERG, an individual, demands replevin of the property taken from Plaintiff that is currently held by Defendant JOHN DOE, an individual, in the JOHN DOE Wallet Addresses and/or the JOHN DOE Secondary Addresses; and thereby demands that the wrongfully obtained property be restored to Plaintiff.

COUNT III – VIOLATION OF 18 U.S.C. § 1030(a)(2)(C), 1030(a)(4), and 1030(a)(5)(C) (COMPUTER FRAUD AND ABUSE ACT ["CFAA"])

Plaintiff re-alleges, and adopts by reference herein, Paragraphs 1-55 above, and further alleges:

69. This cause of action asserts a claim against JOHN DOE for violations of 18 U.S.C. § 1030(a)(2)(C), 1030(a)(4), and 1030(a)(5)(C) (the "Computer Fraud and Abuse Act") for unauthorized access to a protected computer to obtain information, for knowingly doing so with an intent to defraud, for furthering fraudulent activity thereby to obtain something of value, and for intentionally accessing a protected computer without authorization and causing Plaintiff damage or loss.

70. Plaintiff's cellphone is a "protected computer" as defined in 18 U.S.C. § 1030(e)(2)(B) because it is used in interstate or foreign commerce or communication, including sending and receiving electronic mail, sending and receiving text messages, and accessing and interacting with the internet.

71. JOHN DOE, without authorization, accessed -- knowingly and with intent to defraud Plaintiff -- a protected computer (*i.e.*, Plaintiff's cellphone).

72. As a result of his unauthorized access to Plaintiff's cellphone, JOHN DOE obtained from Plaintiff's cellphone valuable information (*i.e.*, passcodes to/in Plaintiff's e-mail account and BlockFi account).

73. JOHN DOE also intentionally furthered a fraud by obtaining unauthorized access to Plaintiff's protected cellphone so he could falsely assume her identity and access her e-mail account and her BlockFi account to steal from her valuable cryptocurrency assets.

74. In addition, JOHN DOE intentionally accessed Plaintiff's protected computer without authorization; and as a result of such conduct, caused Plaintiff damage or loss.

75. As a consequence of JOHN DOE's unauthorized access to Plaintiff's cellphone and the private information maintained in connection therewith, Plaintiff has suffered damage far in excess of Five Thousand Dollars ($5,000.00).

76. Moreover, as a consequence of JOHN DOE interrupting Plaintiff's service, she has suffered damage far in excess of Five Thousand Dollars ($5,000.00).

WHEREFORE, Plaintiff TULLIA HEISSENBERG, an individual, demands entry of a judgment against Defendant JOHN DOE, an individual, for damages, including compensatory damages, punitive damages, interest, expenses, and any other relief the Court deems just and proper.

COUNT IV - UNJUST ENRICHMENT

Plaintiff re-alleges, and adopts by reference herein, Paragraphs 1 - 55 above, and further alleges:

77. Plaintiff conferred a direct benefit upon JOHN DOE (albeit unwillingly so) by providing the extremely valuable cryptocurrency that JOHN DOE stole from Plaintiff.

78. JOHN DOE has knowledge of the benefit Plaintiff conferred upon him and has retained such benefit.

79. The circumstances under which Plaintiff conferred, and JOHN DOE accepted, such benefit render JOHN DOE's retention of the benefits inequitable.

80. Equity requires that JOHN DOE return to Plaintiff the benefits she conferred upon JOHN DOE.

WHEREFORE, Plaintiff TULLIA HEISSENBERG, an individual, demands entry of a judgment against Defendant JOHN DOE, an individual, for damages, including compensatory damages, punitive damages, interest, expenses, and any other relief the Court deems just and proper

COUNT V – IMPOSITION OF A CONSTRUCTIVE TRUST AND DISGORGEMENT OF FUNDS

Plaintiff re-alleges, and adopts by reference herein, Paragraphs 1 - 55 above, and further alleges:

81. This is an action to impose a constructive trust upon the property taken from Plaintiff that is currently held by JOHN DOE in the JOHN DOE Wallet Addresses and/or the JOHN DOE Secondary Addresses.

82. This action further calls for the restoration to Plaintiff of that wrongfully obtained property.

83. As set forth above, JOHN DOE -- through actual fraud, misappropriation, conversion, theft, or other questionable means -- obtained Plaintiff's cryptocurrency, which in equity and good conscience JOHN DOE should not be permitted to hold.

84. The cryptocurrency assets at issue are specific, identifiable property and can be traced in assets of JOHN DOE's at the JOHN DOE Wallet Addresses and/or the JOHN DOE Secondary Addresses.

85. Any and all assets being held by JOHN DOE in the JOHN DOE Wallet Addresses and the JOHN DOE Secondary Addresses must be held in trust for Plaintiff's benefit, as JOHN DOE is not entitled to the benefit of wrongfully misappropriated, converted, and stolen funds and cryptocurrency assets that were taken from Plaintiff.

86. The 28.0265 BTC and 1108 ETH identified herein which are being held by JOHN DOE in the JOHN DOE Wallet Addresses and/or the JOHN DOE Secondary Addresses must be disgorged to Plaintiff's benefit, as JOHN DOE is not entitled to the benefit of wrongfully misappropriated, converted, and stolen funds and cryptocurrency assets that were taken from Plaintiff.

WHEREFORE, Plaintiff TULLIA HEISSENBERG, an individual, demands the equitable imposition of a constructive trust over the property taken from Plaintiff that is currently held by Defendant JOHN DOE, an individual, in the JOHN DOE Wallet Addresses and/or the JOHN DOE Secondary Addresses; and further demands that the wrongfully obtained property be restored to Plaintiff.

DEMAND FOR JURY TRIAL

Plaintiff hereby demands a trial by jury on all claims so triable.

RESERVATION OF RIGHTS

Plaintiff reserves her right to further amend this Complaint, upon completion of her investigation and discovery, to assert any additional claims for relief against Defendants or other parties as may be warranted under the circumstances and as allowed by law.

Respectfully submitted,

SILVER MILLER
11780 W. Sample Road
Coral Springs, Florida 33065
Telephone: (954) 516-6000

By: _____
DAVID C. SILVER
E-mail: DSilver@SilverMillerLaw.com
JASON S. MILLER
E-mail: JMiller@SilverMillerLaw.com

Counsel for Plaintiff Tullia Heissenberg

Dated: April 14, 2021