

**UNITED STATES DISTRICT COURT
MIDDLE DISTRICT OF FLORIDA**

Civil Action No. _____

WILLIAM ROSE, an individual,
Plaintiff,

v.

CELLULAR TOUCH WIRELESS, INC., a Florida corporation;
Defendant.

COMPLAINT FOR DAMAGES AND EQUITABLE RELIEF

Plaintiff WILLIAM ROSE, an individual (hereafter referred to as “Plaintiff”), by and through undersigned counsel, hereby sues Defendant CELLULAR TOUCH WIRELESS, INC., a Florida corporation; for damages and equitable relief. As grounds therefor, Plaintiff alleges the following:

PRELIMINARY STATEMENT

1. This action is brought by Plaintiff, a Metro by T-Mobile subscriber who lost approximately Two Hundred Eighty Thousand Dollars (\$280,000.00) worth of cryptocurrency in August 2021 in an under-recognized 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 three hundred (300) victims of unauthorized SIM swapping 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. Defendant is an Authorized Dealer who operates retail store locations in Florida under the brand of cellular telecommunications provider Metro by T-Mobile -- the telecom provider through whom Plaintiff received his monthly cellphone service.

5. Documents maintained by Metro by T-Mobile and by Defendant demonstrate that employees or employee credentials at a Defendant store location were used to effectuate the unauthorized SIM swap imposed upon Plaintiff, which was vital in the scheme to steal Plaintiff's assets.

6. But for the Metro by T-Mobile Authorized Dealer's intentional participation in the scheme or its recklessness and gross negligence in failing to adequately protect employee credentials and Plaintiff's personal identifying information/Metro by T-Mobile account, Plaintiff would not have suffered the harm that he did.

7. Plaintiff brings this lawsuit to compensate him for his losses.

PARTIES, JURISDICTION AND VENUE

THE PARTIES

Plaintiff

8. Plaintiff WILLIAM ROSE is an individual domiciled in Mansfield, Massachusetts, is a citizen of the state of Massachusetts, and is *sui juris*. At all times relevant hereto, Plaintiff was an accountholder and subscriber with Metro

by T-Mobile. Among other things, Plaintiff's subscription with Metro by T-Mobile permitted Plaintiff to use his cellphone for the following -- all of which Plaintiff in fact did with his phone: make and receive telephone calls with people around the world, send and receive text messages with people around the world, and access the internet and websites around the world through one or more web browsers.

Defendant

9. Defendant CELLULAR TOUCH WIRELESS, INC. ("Defendant" or "CELLULAR TOUCH WIRELESS") is a corporation organized under the laws of Florida with its principal place of business in Tampa, FL. CELLULAR TOUCH WIRELESS is a Metro by T-Mobile Authorized Dealer that operates under the Metro by T-Mobile brand. CELLULAR TOUCH WIRELESS operates numerous Metro by T-Mobile Authorized Dealer stores, including one at 3369 Dr. Martin Luther King Jr. Blvd. in Fort Myers, Florida.

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) his 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. Along with 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 him to name these persons or entities as party defendants. By not naming such persons or entities at this time, Plaintiff is not waiving his right to amend this pleading to add such parties, should the facts warrant adding such parties.

JURISDICTION AND VENUE

12. This Court has original jurisdiction over the subject matter of this action pursuant to 28 U.S.C. § 1331, because the matter in controversy arises under the laws of the United States.

13. This Court also has supplemental jurisdiction over the state law claims pursuant to 28 U.S.C. § 1367.

14. This Court has personal jurisdiction over Defendant because it: (a) conducts business in this jurisdiction, and (b) committed a tort upon Plaintiff 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

Metro by T-Mobile's Business, Authorized Dealer Stores, and Customer Assurances

16. Metro by T-Mobile is a wholly-owned subsidiary of T-Mobile USA, Inc., which is the United States operating entity of T-Mobile International A.G. & Co., the mobile communications subsidiary of Deutsche Telekom AG & Co. K.G. Metro by T-Mobile provides wireless service to subscribers in the United States, Puerto Rico, and the U.S. Virgin Islands.

17. Metro by T-Mobile markets and sells wireless telephone service through standardized wireless service plans at various retail locations, online, and over the telephone.

18. Among the retail locations at which accountholders can get customer service in person are: (1) T-Mobile/Metro corporate-owned stores, and (2) Authorized Dealer stores. To accountholders, the difference between the two is functionally imperceptible. Both kinds of stores share inventory with one another, use the same computer systems and databases, market themselves under the T-Mobile/Metro brand, and obtain corporate training from T-Mobile/Metro together. Defendant in the instant matter operates numerous Metro by T-Mobile Authorized Dealer stores.

19. In connection with its wireless services, Metro by T-Mobile maintains wireless accounts enabling its customers to have access to information about the services they purchase from Metro by T-Mobile. That access is available at Metro

by T-Mobile Authorized Dealer stores just as it is available at Metro by T-Mobile Authorized Dealer corporate-owned stores.

20. It is widely recognized that mishandling of customer wireless accounts can facilitate identify theft and related consumer harms.

21. Among other things, Metro by T-Mobile's sales and marking materials state: **"We have implemented various policies and measures to ensure that our interactions are with you or those you authorize to interact with us on your behalf – and not with others pretending to be you or claiming a right to access your information."** (Emphasis added).

22. Metro by T-Mobile's sales and marking materials further state that, unless Metro by T-Mobile can verify someone's identity through certain personal information or a PIN if requested by the customer, Metro by T-Mobile's policy is not to release any account-specific information.

Verification of Your Identity We have to verify your identity before we can give you access to or delete your personal data. If we can't verify your identity, we'll unfortunately have to deny your request. This is to protect you. To learn more about our verification process, please read our [FAQs](#). Enterprise customer accounts (T-Mobile for Business/ T-Mobile for Government) are protected through authentication and access methods that are different than those used by individual consumers.

23. Despite these statements and other similar statements, Metro by T-Mobile Authorized Dealer stores -- much like Metro by T-Mobile corporate-owned stores themselves -- often fail to provide reasonable and appropriate security to prevent unauthorized access to customer accounts.

24. Under Metro by T-Mobile's procedures, an unauthorized person -- including Metro by T-Mobile Authorized Dealers' own agents and employees acting without the customer's permission -- can easily impersonate the identity of the accountholder and then access and make changes to all the information that a legitimate customer could access and to which the customer could make changes if the customer were so authorized. For example, a simple Google search may reveal the information used to verify the identity of an accountholder, such as an address, ZIP Code, telephone number, and/or e-mail address.

How SIM Swapping Works

25. "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.

26. 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.

27. Generally, “SIM swapping” refers to a method of unauthorized takeover of a victim’s wireless account by malicious actors, 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:



28. SIM swaps are commonly executed by attackers who gain authorized or 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.

29. Often working in tandem with a telecommunications provider’s employees and authorized agents -- 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, walks into a telecommunications provider's retail store, or gains direct access to the telecom provider's customer service computer network intent on assuming the electronic identity of the target of the crime by possessing and utilizing information that only the telecommunications provider should have.

30. 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.

31. 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.

32. As discussed above, in some cases, upon information and belief, telecommunications provider employees and authorized agents 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.

33. 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.

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

35. 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]).

36. 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.

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

38. 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 while simultaneously denying their accountholders their power over such things.

The Anatomy of Plaintiff's SIM Swap

39. In the instant matter, insiders at the defendant Metro by T-Mobile Authorized Dealer -- whether acting as a co-conspirators to the theft or through abject negligence -- transferred to an unknown John Doe control over Plaintiff's mobile telephone number and e-mail address, which led to the swift theft of approximately Two Hundred Eighty Thousand Dollars (\$280,000.00) in cryptocurrency assets from Plaintiff on or about August 14, 2021.

40. **On the evening of August 13, 2021**, a representative(s) of Metro by T-Mobile Authorized Dealer CELLULAR TOUCH WIRELESS in Fort Myers, FL 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. Plaintiff was with his wife in Ames, Iowa on August 13, 2021 celebrating her grandparents' 65th wedding anniversary -- thousands of miles

away from Fort Myers, FL when the SIM card transfer was processed -- and he did not authorize the transfer.

42. Not only did Plaintiff suffer the theft of his identity and control over his SIM card and cellular telephone number, the unauthorized SIM card transfer produced a hack into his bank account and the theft of cryptocurrency he held.

43. In the aftermath of learning that his SIM card had been transferred without his authorization and that he had financial/cryptocurrency assets stolen from him, Plaintiff contacted Metro by T-Mobile to regain access over his SIM card and phone number and to obtain information on how the unauthorized SIM swap occurred.

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

45. The Metro by T-Mobile telephone customer service representative with whom Plaintiff spoke confirmed for Plaintiff that his unauthorized SIM swap took place in a Metro by T-Mobile store and that it was a "malicious act"; however, despite Plaintiff's pointed inquiries seeking information about who processed the unauthorized SIM swap and at what retail store it took place, Metro by T-Mobile did not provide him that information.


46. Metro by T-Mobile updated the PIN/passcode previously enacted on Plaintiff's telephone account, told Plaintiff that he would be afforded the highest level of security on his account, and assured Plaintiff that no future unauthorized SIM transfers would be allowed.

John Doe’s Theft of Plaintiff’s Cryptocurrency Holdings

47. Provided access by Defendant’s employees or authorized agents, John Doe -- working with those employees and/or agents -- was able to access Plaintiff’s cellphone and Plaintiff’s cryptocurrency wallet at MyEtherWallet, where Plaintiff stored a valuable cryptocurrency portfolio.

48. Defendant worked to allow John Doe (who may or may not be an employee or authorized agent of Defendant) to maliciously gain access to Plaintiff’s personal identifying information, confidential information of his stored on the Metro by T-Mobile network, and his cryptocurrency accounts.

49. At or about August 14, 2021 at 02:38 a.m. +UTC, John Doe withdrew from Plaintiff’s MyEtherWallet account the following cryptocurrency assets without Plaintiff’s knowledge or authorization, *to wit*:

Name: William Rose			
August 13, 2021 9:31 p.m.		Unauthorized transfer of Mr. Rose’s SIM card	
Date/Time of Cryptocurrency Theft	Cryptocurrency Assets Stolen	Location from which Assets were Stolen	Approximate Value of Funds/Assets Stolen as of Date of Theft ¹ [August 14, 2021]
August 14, 2021 2:38 a.m. +UTC	1,800.6460144713 Quant (QNT)	MyEtherWallet	\$280,414.60
TOTAL			\$280,414.60

¹ Valuation of the stolen funds/assets is calculated using market data compiled by www.CoinMarketCap.com, which takes the volume weighted average of all prices reported at several dozen cryptocurrency markets serving investors in the United States and abroad.

50. As of the date on which they were taken from him, the 1,800.6460144713 QNT stolen from Plaintiff were valued at approximately Two Hundred Eight Thousand Dollars (\$280,000.00).

51. Plaintiff has also learned that the IMEI used by the John Doe thief with whom Defendant coordinated the unauthorized transfer of Plaintiff's SIM card was used in numerous other SIM swaps at or about the same time as Plaintiff's SIM swap -- thus demonstrating that Plaintiff's harm was not an isolated incident and should have been flagged in, and prevented by, Defendant and Metro by T-Mobile's security systems.

52. Upon further information and belief, Defendant was aware that its security systems and internal software platform contained significant holes and weaknesses that permitted unchecked security bypasses and allowed unauthorized actors to enter the system and gain control over customer accounts and information; yet Defendant did not take adequate measures to address those holes and weaknesses.

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 his 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 his rights, Plaintiff has retained undersigned counsel and is obligated to pay counsel a reasonable fee for its services.

COUNT I – BREACH OF FEDERAL COMMUNICATIONS ACT
[47 U.S.C. §§ 206, 222]
(UNAUTHORIZED DISCLOSURE OF CUSTOMER CONFIDENTIAL
PROPRIETARY INFORMATION AND PROPRIETARY NETWORK
INFORMATION)

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

56. Metro by T-Mobile is a “common carrier” engaging in interstate commerce by wire regulated by the Federal Communications Act (“FCA”) and subject to the requirements, *inter alia*, of sections 206 and 222 of the FCA.

57. Defendant is an authorized agent of common carrier Metro by T-Mobile and, under section 217 of the FCA [47 U.S.C. § 217], is itself liable for adhering to the requirements of the FCA as well as its violations of the FCA.

58. Under section 206 of the FCA [47 U.S.C. § 206], “[i]n case any common carriers shall do, or cause or permit it to be done, any act, matter, or thing in this chapter prohibited or declared to be unlawful, or shall omit to do any act, matter, or thing in this chapter required to be done, such common carrier shall be liable to the person or persons injured thereby for the full amount of damages sustained in consequence of any such violation of the provisions of this chapter, together with a reasonable counsel or attorney’s fee, to be fixed by the court in every case of recovery, which attorney’s fee shall be taxed and collected as part of the costs in the case.”

59. Section 222(a) of the FCA [47 U.S.C. § 222(a)] requires every telecommunications carrier to protect, among other things, the confidentiality of proprietary information of, and relating to, customers (“CPI”).

60. Section 222(c)(1) of the FCA [27 U.S.C. § 222(c)(1)] further requires that, “[e]xcept as required by law or with the approval of the customer, a telecommunications carrier that receives or obtains customer proprietary information by virtue of its provision of a telecommunications service shall only use, disclose, or permit access to customer proprietary network information [‘CPNI’] in its provision of (A) telecommunications services from which such information is derived, or (B) services necessary to or used in the provision of such telecommunication services”

61. The information disclosed to hackers by Defendant in the August 2021 SIM swap fraud transferring Plaintiff’s telephone number was CPI and CPNI under Section 222 of the FCA.

62. Defendant failed to protect the confidentiality of Plaintiff’s CPI and CPNI, including his wireless telephone number, account information, and his private communications, by divulging that information to hackers on or about August 13, 2021.

63. Through its negligence, gross negligence and deliberate acts, including inexplicable failures to follow its own security procedures; supervise its employees; the CPNI Regulations; Metro by T-Mobile’s Privacy Policy, COBC, and CPNI Policy; and by allowing its employees to bypass such procedures, Defendant

permitted hackers to access Plaintiff's telephone number, telephone calls, text messages and account information to steal approximately \$280,000.00 worth of his cryptocurrency.

64. As a direct consequence of Defendant's violations of the FCA, Plaintiff has been damaged by loss of approximately \$280,000.00 worth in cryptocurrency which Defendant allowed to fall into the hands of thieves, and for other damages in an amount to be proven at trial in this matter.

65. Plaintiff is also entitled to his attorney's fees under the FCA in bringing this action against Defendant for its gross negligence and fraudulent misrepresentation as to the security that it was obligated to provide for customer accounts as required by the FCA and the CPNI Regulation.

COUNT II – VIOLATION OF 18 U.S.C. § 1030(a)(2)(C) and 1030(a)(4)
(COMPUTER FRAUD AND ABUSE ACT [“CFAA”])

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

66. This cause of action asserts a claim against Defendant for violations of 18 U.S.C. § 1030(a)(2)(C) and 1030(a)(4) (the “Computer Fraud and Abuse Act”) for aiding and abetting authorized access to a protected computer to obtain information, for knowingly doing so with an intent to defraud, and for furthering fraudulent activity thereby to obtain something of value.

67. 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.

68. Defendant aided and abetted an unauthorized and unknown person by granting to that person, acting knowingly and with intent to defraud Plaintiff, access to a protected computer (*i.e.*, Plaintiff's cellphone).

69. Defendant divulged to an unauthorized person Plaintiff's personal identifying information -- including his private security PIN codes -- and transferred to that unauthorized person Plaintiff's cellphone number and the telecommunications services tied thereto through Plaintiff's cellphone.

70. Defendant aided and abetted the unauthorized transfer of Plaintiff's SIM card despite the clear barrier of numerous security protocols on Plaintiff's account that Defendant overtly ignored and bypassed -- a barrier put in place to prevent an unauthorized SIM swap.

71. As a consequence of Defendant's actions and omissions, Plaintiff has suffered damage far in excess of Five Thousand Dollars (\$5,000.00).

72. Moreover, as a consequence of Defendant interrupting Plaintiff's service, he has suffered damage far in excess of Five Thousand Dollars (\$5,000.00) to respond to the SIM swap inflicted upon him, investigate this matter, and assess his damages.

73. Included among the costs he has incurred are fees exceeding Five Thousand Dollars (\$5,000.00) to retain the ongoing services of a cryptographic tracing expert to trace blockchain movements of Plaintiff's stolen assets as a means

of identifying where they traveled once they were taken from Plaintiff's possession and who possesses those stolen assets. Had Defendant not interrupted Plaintiff's service during the critical time in which Plaintiff's assets were stolen, Plaintiff would not have incurred such consequential costs.

COUNT III – VIOLATION OF 18 U.S.C. § 1030(a)(6)
(COMPUTER FRAUD AND ABUSE ACT [“CFAA”])

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

74. This cause of action asserts a claim against Defendant for violations of 18 U.S.C. § 1030(a)(6) (the “Computer Fraud and Abuse Act”) for knowingly and with an intent to defraud trafficking in Plaintiff's password or similar information through which a computer may be accessed without authorization where such trafficking affects interstate commerce.

75. Defendant knowingly, and with intent to defraud Plaintiff, trafficked in Plaintiff's password or similar information by giving Plaintiff's security passcode to an unauthorized third party.

76. Using Plaintiff's passcode, the unauthorized third party was able to access Plaintiff's computer (*i.e.*, his cellphone) without Plaintiff's authorization.

77. The unauthorized access to Plaintiff's cellphone affects interstate commerce, as the phone can be used -- and is regularly used -- as a tool to make interstate phone calls, access the internet for the purchase and sale of goods and services, and transmit text and data across state lines using electronic mail and text messaging services.

78. As a consequence of the conduct described above -- and because Defendant interrupted Plaintiff's service during a critical timeframe -- Plaintiff has suffered damage.

COUNT IV – VIOLATION OF FLA. STAT. §§ 815.01, et seq.
(FLORIDA COMPUTER CRIMES ACT)

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

79. This cause of action asserts a claim against Defendant for violations of Fla. Stat. §§ 815.01, *et seq.* (the Florida Computer Crimes Act [“the Act”]) for aiding and abetting unlawful access to Plaintiff's Metro by T-Mobile cellphone and for disrupting and denying Plaintiff's Metro by T-Mobile service in a manner that allowed the theft of his cryptocurrency assets.

80. Fla. Stat. § 815.06 deems a person to have committed an offense under the Act if he/she/it, *inter alia*:

- (a) Accesses or causes to be accessed any computer, computer system, computer network, or electronic device with knowledge that such access is unauthorized
- (b) Disrupts or denies or causes the denial of the ability to transmit data to or from an authorized user of a computer, computer system, computer network, or electronic device, which, in whole or in part, is owned by, under contract to, or operated for, on behalf of, or in conjunction with another.

81. Furthermore, Fla. Stat. § 815.06 provides a civil right of action to someone aggrieved by a violation of any provision of the Act; and the aggrieved person is authorized to sue therefor and recover compensatory damages as well as reasonable attorneys' fees incurred.

82. Under Fla. Stat. § 815.03(4), the wireless telecommunications network for which Plaintiff paid a monthly subscription to access from Metro by T-Mobile is deemed a “computer network.”

83. Under Fla. Stat. § 815.03(6), the wireless telecommunications services for which Plaintiff paid a monthly subscription to Metro by T-Mobile are deemed “computer services.”

84. Under Fla. Stat. § 815.03(9), Plaintiff’s cellphone is deemed an “electronic device.”

85. At the time Defendant handed over to an unauthorized person Plaintiff’s cellphone number, Plaintiff’s password, an identifying code, Plaintiff’s personal identification number, or other confidential information and control over Plaintiff’s cellular telephone services, Defendant not only allowed the unauthorized person access to Plaintiff’s cellular telephone services but also prevented Plaintiff’s authorized access to those same services during the critical time period in which the theft of Plaintiff’s assets took place.

86. To the extent Defendant did not commit primary violations of this statute, Defendant provided vital assistance and aided and abetted violation of the statute by the unauthorized person -- who did so knowingly and without authorization or without reasonable grounds to believe that he or she had such authorization to access Plaintiff’s cellular telephone.

87. Through its knowing cooperation with the hacker in the SIM swap fraud, Defendant provided the hacker with means to access Plaintiff's cellphone to steal nearly \$280,000.00 worth of cryptocurrency from Plaintiff.

COUNT V – NEGLIGENCE

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

88. Defendant owed a duty to Plaintiff to exercise reasonable care in safeguarding and protecting his Personal Information, including CPI and CPNI, and keeping it from being compromised, lost, stolen, misused and/or disclosed to unauthorized parties.

89. This duty included, among other things, designing, maintaining, and testing its security systems to ensure that Plaintiff's Personal Information, including CPI and CPNI, was adequately secured and protected.

90. Defendant knew that Plaintiff's Personal Information, including CPI and CPNI, was confidential and sensitive.

91. Indeed, Metro by T-Mobile acknowledged that in its Privacy Policy, COBC, and CPNI Policy.

92. Defendant likewise knew that Plaintiff's Personal Information was vulnerable to hacks by thieves and other criminals because, *inter alia*, Metro by T-Mobile acknowledged such in its Privacy Policy, COBC, and CPNI Policy.

93. Defendant thus knew of the substantial and foreseeable harms that could occur to Plaintiff if Defendant did not place adequate security on Plaintiff's

Personal Information and did not follow its own security measures for Plaintiff's account.

94. Having been entrusted by Plaintiff to safeguard his Personal Information, including CPI and CPNI, Defendant had a special relationship with Plaintiff.

95. Plaintiff signed up for Metro by T-Mobile's wireless services and agreed to provide his Personal Information to Metro by T-Mobile with the understanding that Metro by T-Mobile and its agents would take appropriate measures to protect it. But Defendant -- acting as an authorized agent of Metro by T-Mobile -- did not protect Plaintiff's Personal Information and violated his trust.

96. Defendant knew its security was inadequate.

97. Moreover, Defendant should have recognized that the IMEI number to which Plaintiff's SIM card was transferred had been used in numerous other unauthorized SIM card transfers and should have flagged or blacklisted it as a destination IMEI number. To the extent Defendant failed to recognize that or did recognize it yet failed to prevent the unauthorized SIM swap perpetrated upon Plaintiff, Defendant breached its duty of care and should be held liable.

98. Defendant is morally culpable, given prior security breaches involving its own employees and flawed software system and the multiple times that the IMEI number to which Plaintiff's SIM card was transferred had been used in numerous other unauthorized SIM card transfers.

99. Defendant breached its duty to exercise reasonable care in safeguarding and protecting Plaintiff's Personal Information, including CPI and CPNI, by failing to adopt, implement, and maintain adequate security measures to safeguard that information, including its duty under the FCA, the CPNI Rules, and its own Privacy Policy, COBC, and CPNI Policy.

100. Defendant's failure to comply with federal and state requirements for security further evidences Defendant's negligence in failing to exercise reasonable care in safeguarding and protecting Plaintiff's Personal Information, including CPI and CPNI.

101. But for Defendant's wrongful and negligent breach of the duties owed to Plaintiff, his Personal Information, including his CPI and CPNI, would not have been compromised, stolen, viewed, and used by unauthorized persons.

102. Defendant's negligence was a direct and legal cause of the theft of Plaintiff's Personal Information and the legal cause of his resulting damages, including, but not limited to, the theft of approximately \$280,000.00 worth of cryptocurrency.

103. The injury and harm suffered by Plaintiff was the reasonably foreseeable result of Defendant's failure to exercise reasonable care in safeguarding and protecting Plaintiff's Personal Information, including his CPI and CPNI.

104. Defendant's misconduct as alleged herein is malice, fraud, or oppression in that it was despicable conduct carried on by Defendant with a willful

and conscious disregard of the rights or safety of Plaintiff and despicable conduct that has subjected Plaintiff to cruel and unjust hardship in conscious disregard of his rights.

105. As a result, Plaintiff is entitled to punitive damages against Defendant.

COUNT VI – NEGLIGENT TRAINING AND SUPERVISION

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

106. Defendant owed Plaintiff a duty to exercise reasonable care in supervising and training its employees to safeguard and protect Plaintiff's Personal Information, including CPI and CPNI, and to keep it from being compromised, lost, stolen, misused and/or disclosed to unauthorized parties.

107. Defendant was aware of the ability of its employees to bypass security measures and the fact that its employees actively participated in fraud involving its customers, including pretexting and SIM card swap fraud, by bypassing such security measures.

108. Defendant knew that Plaintiff's Personal Information, including CPI and CPNI, was confidential and sensitive.

109. Having been entrusted by Plaintiff to safeguard his Personal Information, including CPI and CPNI, Defendant had a special relationship with Plaintiff.

110. Plaintiff signed up for Metro by T-Mobile's wireless services and agreed to provide his Personal Information to Metro by T-Mobile with the

understanding that Metro by T-Mobile's employees and authorized representatives would take appropriate measures to protect it.

111. Metro by T-Mobile also made promises in the Privacy Policy, COBC, and CPNI Policy that its employees and authorized agents would respect its customers' privacy and that Metro by T-Mobile would supervise and train its employees and authorized agents to adhere to its legal obligations to protect their Personal Information.

112. Defendant breached its duty to supervise and train its employees to safeguard and protect Plaintiff's Personal Information, including CPI and CPNI, by not requiring them to adhere to their obligations under the CPNI Rules and other legal provisions.

113. Defendant's employees facilitated a SIM swap fraud on Plaintiff by intentionally bypassing important security measures and not requiring an individual(s) requesting control over Plaintiff's SIM card and telephone number to present valid identification before transferring to that individual(s) control over Plaintiff's SIM card and telephone number.

114. Defendant's employees also allowed the unauthorized SIM swap perpetrated upon Plaintiff to an IMEI number that had been used in numerous other unauthorized SIM card transfers that either was or should have been flagged or blacklisted as a destination IMEI number.

115. Defendant knew its supervision and monitoring of its employees was inadequate through its knowledge from prior incidents that its own and/or fellow Metro by T-Mobile employees cooperated with hackers in SIM swap fraud.

116. Defendant breached its duty to exercise reasonable care in supervising and monitoring its employees to protect Plaintiff's Personal Information, including CPI and CPNI.

117. Defendant's failure to comply with the requirements of the FCA and CPNI Rules further evidence Defendant's negligence in adequately supervising and monitoring its employees so that they would safeguard and protect Plaintiff's Personal Information, including CPI and CPNI.

118. But for Defendant's wrongful and negligent breach of its duties to supervise and monitor its employees, Plaintiff's CPI and CPNI would not have been disclosed to unauthorized individuals through SIM swap fraud.

119. Defendant's negligence was a direct and legal cause of the theft of Plaintiff's Personal Information and the legal cause of his resulting damages, including, but not limited to, the theft of approximately \$280,000.00 worth of cryptocurrency.

120. The injury and harm suffered by Plaintiff was the reasonably foreseeable result of Defendant's failure to supervise and monitor its employees in safeguarding and protecting Plaintiff's Personal Information, including his CPI and CPNI.

121. Defendant's misconduct as alleged here was done with malice, fraud, and oppression in that it was despicable conduct carried on by Defendant with a willful and conscious disregard of the rights or safety of Plaintiff and despicable conduct that has subjected Plaintiff to cruel and unjust hardship in conscious disregard of his rights. As a result, Plaintiff is entitled to punitive damages against Defendant.

COUNT VII – CIVIL CONSPIRACY

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

122. Defendant, by and through its authorized agents, agreed and combined with yet-unknown third-party thieves to engage in a conspiracy to:

- (a) violate federal laws, including the Federal Communications Act;
- (b) hand over to unauthorized persons Plaintiff's cellphone number, Plaintiff's Metro by T-Mobile password/identifying code, Plaintiff's personal identification number, or other confidential information and control over Plaintiff's cellular telephone services;
- (c) overtly and intentionally ignore and bypass numerous security protocols on Plaintiff's account -- barriers expressly represented to Plaintiff that were put in place to prevent an unauthorized SIM swap;
- (d) prevent Plaintiff's authorized access to the Metro by T-Mobile services for which he paid during the critical time period in which the theft of Plaintiff's assets took place; and
- (e) represent and support a criminal syndicate aimed at stealing cryptocurrency from Metro by T-Mobile accountholders (including Plaintiff) following unauthorized SIM swaps on those Metro by T-Mobile accountholders.

123. The participants in the conspiracy put their own pecuniary interests ahead of the welfare and economic safety of the victim of this portion of the conspiracy.

124. Defendant failed to comply with its legal obligations -- and in fact intentionally or through recklessness and gross negligence violated those obligations -- and enabled the illegal activity inflicted upon Plaintiff.

125. Defendant acted in concert in furtherance of its role in the common plan to steal, launder, and dissipate cryptocurrency assets from Metro by T-Mobile accountholders, including Plaintiff.

126. As a direct and proximate result of Defendant's participation in, and furtherance of, the conspiracy; Plaintiff has suffered damages.

PRAYER FOR RELIEF

WHEREFORE, Claimant WILLIAM ROSE, an individual, respectfully prays for relief as follows:

- (a) A judgment awarding Plaintiff equitable restitution, including, without limitation, restoration of the *status quo ante*, and return to Plaintiff all cryptocurrency or fiat currency taken from him in connection with the SIM card swap intentionally inflicted or negligently allowed by Defendant;
- (b) An award of any and all additional damages recoverable under law including but not limited to compensatory damages, punitive damages, incidental damages, and consequential damages;
- (c) Pre- and post-judgment interest;
- (d) Attorneys' fees, expenses, and the costs of this action; and
- (e) All other and further relief as the Court deems necessary, just, and proper.

DEMAND FOR JURY TRIAL

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

RESERVATION OF RIGHTS

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

Respectfully submitted,

SILVER MILLER

4450 NW 126th Avenue - Suite 101
Coral Springs, Florida 33065
Telephone: (954) 516-6000

By: /s/ David C. Silver

DAVID C. SILVER

Florida Bar No. 572764

E-mail: DSilver@SilverMillerLaw.com

JASON S. MILLER

Florida Bar No. 072206

E-mail: JMiller@SilverMillerLaw.com

Counsel for Plaintiff William Rose

Dated: January 11, 2023