IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLORADO

Case No.: _____

ANDREW SCHOBER,

Plaintiff,

v.

BENEDICT THOMPSON, OLIVER READ, EDWARD J. THOMPSON, CLAIRE L. THOMPSON, PAUL READ, and HAZEL DAVINA WELLS,

Defendants.

COMPLAINT AND JURY TRIAL DEMAND

NATURE OF THE ACTION

1. This case involves theft of Bitcoin currently worth approximately $1 million. Defendants created and deployed "clipboard hijacking" malware (the "Malware") and then used it to steal 16.4552 bitcoins from a computer belonging Plaintiff Andrew Schober.

2. Defendants Benedict Thompson ("Benedict") and Oliver Read ("Oliver") are, on information and belief, friends and/or associates of one another, who communicate and exchange data via the internet. Both Benedict and Oliver are skilled software developers and computer science students. Both were minors when they engaged in the actions and omissions described herein.

3. The deployment of the Malware on Mr. Schober's computer and the subsequent theft of Mr. Schober's cryptocurrency was devastating for Mr. Schober. He

did not eat or sleep for days afterward and has been in a severe state of distress for the past three years. The cryptocurrency accounted for approximately 95% of his net wealth at the time it was stolen from him. Mr. Schober was planning to use the proceeds from his eventual sale of the cryptocurrency to help finance a home and support his family.

4. Recognizing the harms that arise from thefts of personal property, distribution and dissemination of malware, and accessing and using sensitive information without the owner's consent, federal and state laws prohibit such conduct to protect the property and sensitive information of the citizens of the United States and Colorado. Defendants broke those laws.

5. Mr. Schober brings this action to hold Defendants accountable for their violations of federal and state law, and to seek recovery for the grave financial and personal harm he suffered.

THE PARTIES

6. Plaintiff Andrew Schober is, and at all relevant times was, a resident of Colorado.

7. Defendant Benedict Thompson is a resident of Southampton, Hampshire, United Kingdom. He is currently studying Computer Science at the University of Warwick.

8. Defendant Oliver Read is a resident of Bradford, West Yorkshire, United Kingdom. Defendant Read is, or at all relevant times was, also known by the online aliases "Rad3onx" and "Swagoi," among others. He studied Computer Science at Greenhead College in the United Kingdom.

9. Defendant Edward J. Thompson is a resident of Southampton, Hampshire, United Kingdom. He is the father of Defendant Benedict Thompson and the husband of Defendant Claire L. Thompson.

10. Defendant Claire L. Thompson is a resident of Southampton, Hampshire, United Kingdom. She is the mother of Defendant Benedict Thompson and the wife of Defendant Edward J. Thompson.

11. Defendant Paul Read is a resident of Bradford, West Yorkshire, United Kingdom. He is the father of Defendant Oliver Read and the husband of Defendant Hazel D. Wells.

12. Defendant Hazel Davina Wells is a resident of Bradford, West Yorkshire, United Kingdom. She is the mother of Defendant Oliver Read and the wife of Defendant Paul Read.

JURISDICTION AND VENUE

13. This Court has jurisdiction over this matter under 28 U.S.C. § 1332(a)(2) because the amount in controversy exceeds $75,000 (exclusive of costs and interest) and the Plaintiff is completely diverse from Defendants, as Plaintiff is a resident of Colorado and each of the Defendants is a resident of the United Kingdom.

14. The Court has supplemental jurisdiction under 28 U.S.C. § 1367 over the state law claims because the claims are derived from a common nucleus of operative facts.

15. This Court has personal jurisdiction over each Defendant because Defendants purposefully directed their conduct at Colorado, engaged in conduct that has

and had a direct, substantial, reasonably foreseeable, and intended effect of causing injury to persons in Colorado (including in this District), and purposely availed themselves of the laws of Colorado. Mr. Schober operated his computer in Colorado and suffered his injuries in Colorado by the acts and omissions alleged herein.

16. Venue is proper in this District under 28 U.S.C. § 1391 because a substantial part of the conduct giving rise to Mr. Schober's claims occurred in this District, and Mr. Schober was harmed in this District, where he resides, by the acts and omissions alleged herein.

FACTUAL BACKGROUND

I. Description of the Malware and Benedict and Oliver's Distribution and Use of the Malware to Steal Mr. Schober's Cryptocurrency.

17. The Malware was designed by Defendants Benedict and Oliver to clandestinely install itself on the hard drive of the victim's computer [1] and to monitor the victim's computer activity by secretly requesting that the computer run a pattern-matching algorithm each time the victim used the copy-paste (or "clipboard") function on his computer.

18. A primary purpose of the Malware was to divert cryptocurrency from the victim's cryptocurrency wallet to the thief's cryptocurrency wallet.

19. A cryptocurrency wallet (in this case, a Bitcoin wallet) is an algorithmically generated cryptographic key pair comprising a "public key" and a "private key." A public

[1] This type of malware delivery method is typically referred to as a "Trojan Horse," since the payload is concealed within another (often harmless) file downloaded by the victim from the internet.

key allows the wallet owner to receive cryptocurrency from other wallets. A private key allows the wallet owner to send cryptocurrency from his or her wallet to other wallets.

20. Cryptocurrency wallets are required to send and receive transactions on cryptocurrency blockchains. A cryptocurrency wallet is controlled by any entity with control of the private key(s) corresponding to the wallet's public key(s). Anyone who controls a wallet's private key(s) controls the cryptocurrency associated with the wallet.

21. The Malware utilized a "Man-in-the-Middle" attack vector. A Man-in-the-Middle attack is a cyberattack where the attacker secretly intercepts and/or alters the communications between two parties who believe they are directly communicating with one another.

22. Here, Mr. Schober believed he was communicating only with his own cryptocurrency wallet,[2] but because of the Malware, either Benedict or Oliver or both intercepted and altered the communications between Mr. Schober and the Bitcoin blockchain.

23. The Malware worked as follows:

a. Upon detecting that the victim used his or her computer's clipboard function to copy a cryptocurrency wallet address, the Malware automatically inserted a different pre-generated address, selected from within the Malware code, that closely resembled the multi-character wallet address copied by the victim.

b. The Malware then manipulated the victim's computer system by causing the computer to replace the victim's intended wallet address with a wallet address stored in the Malware and controlled by the thief.

[2] Through the "Electrum," software, *infra*, which provides a gateway that allows users of the software to communicate with the validators of the Bitcoin blockchain.

c. By replacing the victim's intended wallet address with an address embedded in the Malware, the thief was able to gain control of the cryptocurrency, because the thief controlled the private key(s) associated with the public key(s) of the wallet address where the cryptocurrency was unintentionally sent as a result of the Malware.

24. A public key is similar to a locked mailbox, and a private key is like the key that unlocks the mailbox – anyone can put mail into a locked mailbox, but only the person with the key can take mail out of the mailbox. By this analogy, Mr. Schober was attempting to send "mail" to a "mailbox" he owned; one or more of the Defendants altered the delivery address prior to Mr. Schober sending the "mail," which caused the "mail" to be delivered to the Defendants' mailbox rather than to Mr. Schober's own "mailbox."[3]

25. Mr. Schober's computer became infected with the Malware after Benedict or Oliver or both posted a link to software—which Defendant(s) called "Electrum Atom"—on the popular public online forum Reddit. The Malware was hidden within this "Electrum Atom" software.

26. "Electrum" is a popular and widely used software client application that hosts cryptocurrency wallets. According to public online posts by at least one of the Defendants, Electrum Atom was a new version of Electrum that would provide users access to a new cryptocurrency called "Bitcoin Atom." In actuality, Electrum Atom was

[3] Cryptocurrency addresses are significantly more complicated than physical addresses. The false addresses used by the Defendants were akin to a situation where a victim had addressed his mail but before the victim placed the mail in his outgoing mailbox the thief changed the recipient address to the thief's address – i.e., changing the address from "John Doe, P.O. Box 12345, Washington, MA 01223" to "John Doe, P.O. Box 12345, Washington, MD, 21733."

nothing more than a malicious version of the Electrum software that functioned as a Trojan Horse for the Malware.

27. As soon as the Malware was installed on Mr. Schober's hard drive, the Malware began monitoring his computer activity.

28. When the Malware recognized that Mr. Schober copied a cryptocurrency wallet address, the Malware immediately executed code that replaced the address he copied with a new address controlled by one or more of the Defendants.

29. In order to identify, match, and replace all possible bitcoin addresses that the victim might copy with a similar-looking bitcoin address controlled by the thief (specifically, an address that matched the first three characters of the intended recipient address), the Malware contained a pre-generated list of 195,112 bitcoin addresses embedded within its code.

30. Each time a victim copied a bitcoin address to his or her computer's clipboard, the Malware replaced the victim's copied address with one of the pre-generated addresses embedded in the Malware.

31. For example, within the amount of time it took the victim to use the clipboard function (i.e., clicking "copy" or using the keyboard command "CRTL-C," and then click "paste" or use the keyboard command "CTRL-P"), the Malware could accomplish the following:

Victim Copies: 1CvXYxmuj7Qs85zWzuUdGBBxcAdeW8729B

Victim Pastes: 1CvXVKevCzW3NeTNWRAbjVthBaFiFTzp7t

Figure 1: The left panel shows the victim's intended recipient address, while the right panel shows the similar-looking, yet subtly different address replaced by the Malware and controlled by the thief.

32. The Malware is particularly intrusive because, once the Malware is installed on the hard drive of the victim's computer, the Malware cannot be deleted from the victim's computer by uninstalling the program in which it was hidden. This is because the Malware embeds itself in the Java library on a victim's computer, regardless of the location where the downloaded file is initially saved, and conceals its existence using an encryption technique that obfuscates the Malware's XOR strings.

33. The Malware is both highly sophisticated and extremely dangerous because it can conceivably be used to copy and replace any information utilized by the clipboard function on any victim's computer (e.g., a version of the Malware could be used to change a victim's password when the victim initiates a password change). Here, the Malware was specifically designed to copy and replace cryptocurrency addresses.[4]

[4] Presumably the Defendants chose to copy and replace cryptocurrency addresses so that they could later launder and obfuscate the proceeds through entirely digital channels prior to spending the cryptocurrency and/or converting the cryptocurrency to fiat currency.

II. Defendants' Intentions and Efforts to Steal, Retain, and Obfuscate Mr. Schober's Cryptocurrency.

34. One or more of the Defendants maintained accounts on at least one online cryptocurrency exchange which had lax or nonexistent Anti-Money Laundering procedures and/or requirements. The online exchange(s) used by the Defendant(s) provided an ideal environment for the Defendant(s) to launder cryptocurrency pilfered with the Malware.

35. Defendants used online exchanges to launder and obfuscate the proceeds prior to spending and/or to converting the cryptocurrency to fiat currency.

36. The Malware developed by Benedict and/or Oliver was downloaded and installed on Mr. Schober's computer in or about January 2018.

37. That same month, 16.4552 bitcoins were stolen from Mr. Schober's computer under transaction ID a6db589147ec24d3d97acf244ac957cbfaeaf145d04c06ec57d782a62c365169.

38. The cryptocurrency stolen from Mr. Schober was immediately sent to the bitcoin wallet address "1CZioyptarnQ3rdT9np2rwMwXftMX9ATT7" (the "Malware Address").

39. Blockchain tracing analyses and investigations revealed that Defendants Benedict and/or Read controlled the Malware Address during the relevant period.

40. The Bitcoin blockchain record shows that in or about February 2018 Mr. Schober's cryptocurrency was transferred from the Malware Address to the Bitfinex deposit address "3CWQ5d2XgCrYuz7F3g4fmhd6VQMv4iPio7" (the "Launder Address"). The Launder Address was hosted on the Bitfinex cryptocurrency exchange.

41. Blockchain tracing analyses and investigations revealed that one or more of the Defendants controlled the Launder Address during the relevant period.

42. Blockchain records indicate that in or about January 2018, approximately 16 bitcoins—which were among the underlying 16.4552 bitcoins stolen from Mr. Schober—were transferred from Mr. Schober's cryptocurrency (Bitcoin) wallet to the Malware Address. *See* Figure 2.

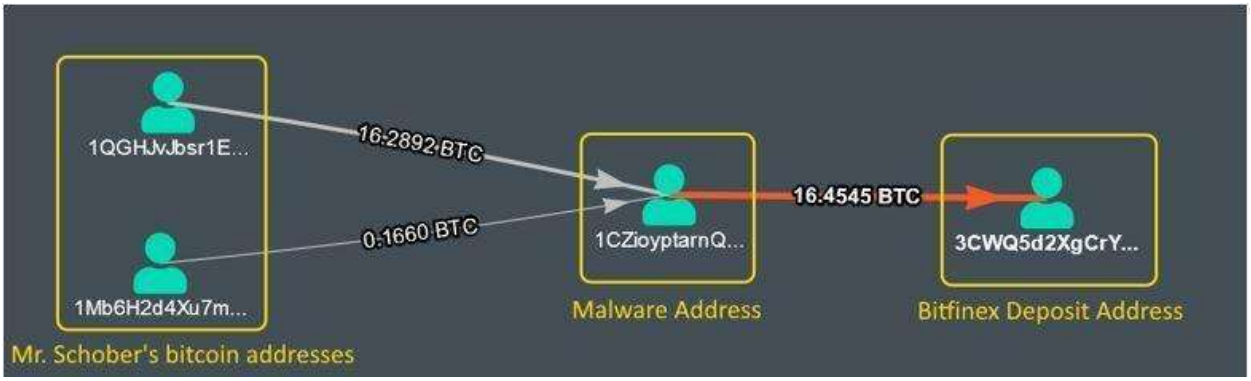


Figure 2: Visual display showing the flow of cryptocurrency from Mr. Schober to the Malware Address to Bitfinex (the Launder Address).

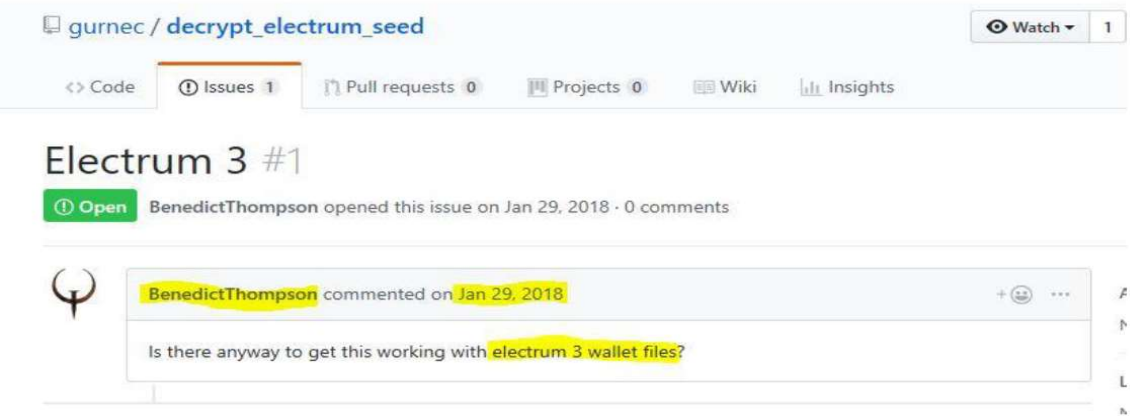
43. Figure 2 shows that the bitcoins stolen from Mr. Schober were sent from Mr. Schober's wallet to the Malware Address.

44. After sending the bitcoins to the Launder Address (labeled the "Bitfinex Deposit Address" in Figure 2), which was hosted on the Bitfinex exchange, Benedict used the Launder Address to convert Mr. Schober's bitcoins to Monero.[5]

[5] Monero is a unique "privacy-focused" cryptocurrency that deliberately obfuscates and anonymizes transactions. Previously, and contrary to the belief of the original authors of the Monero software, Monero transactions could be traced and deanonymized using spatio-temporal analysis techniques.

45. Blockchain analysis revealed at least two apparent connections between the Malware Address and the Launder Address.

46. In or about January 2018, Benedict posted a question on the public online forum, Github, seeking assistance accessing the private key corresponding to the public key of the Malware Address:[6]



III. Defendants' Refusal to Respond to Mr. Schober and Their Parents Responsibility for the Then-Minor Defendant Actions.

47. During the relevant period, Defendant Benedict was under 18 years of age and living with his parents, Defendants Edward J. Thompson and Claire L. Thompson in Southampton, United Kingdom.[7]

48. During the relevant period, Benedict maliciously and/or willfully damaged and/or destroyed personal property belonging to Mr. Schober.

---

[6] Prior to this Github post, Benedict posted on the Github forum only fifteen times during the 2018 calendar year; and this contribution came just hours after Mr. Schober's cryptocurrency was stolen.

[7] Defendants Benedict Thompson, Edward J. Thompson, and Claire L. Thompson are referred to collectively as the "Thompson Defendants."

49. During the relevant period, Defendants Edward J. Thompson and Claire L. Thompson knew or reasonably should have known that their child engaged in illegal computer abuse(s) and/or cryptocurrency theft(s) in a careless and/or reckless manner.

50. Defendants Edward J. Thompson and Claire L. Thompson failed to take reasonable steps to prevent Benedict from causing foreseeable harm resulting from Defendant Benedict's likelihood to continue committing illegal computer abuse(s) and/or cryptocurrency theft(s).

51. In or about December 2019, Mr. Schober emailed a letter to the Thompson Defendants demanding that they return the cryptocurrency stolen from Mr. Schober.

52. As of the date of this Complaint, the Thompson Defendants have not responded to Mr. Schober's request that they return his cryptocurrency.

53. During the relevant period, Oliver was under 18 years of age and living with his parents, Defendants Paul Read and Hazel Davina Wells in Bradford, West Yorkshire, United Kingdom.[8]

54. During the relevant period, Oliver maliciously and/or willfully damaged and/or destroyed personal property belonging to Mr. Schober.

55. During the relevant period, Defendants Paul Read and Hazel Davina Wells knew or reasonably should have known that their child engaged in illegal computer abuse(s) and/or cryptocurrency theft(s) in a careless and/or reckless manner.

[8] Defendants Oliver Read, Paul Read, and Hazel Davina Wells are referred to collectively as the "Read Defendants."

56. Defendants Paul Read and Hazel Davina Wells failed to take reasonable steps to prevent Oliver from causing foreseeable harm resulting from Oliver's likelihood to continue committing illegal computer abuse(s) and/or cryptocurrency theft(s).

57. In or about October 2018, Mr. Schober emailed a letter to the Read Defendants demanding that they return the cryptocurrency stolen from Mr. Schober.

58. As of the date of this Complaint, the Read Defendants have not responded to Mr. Schober's request that they return his cryptocurrency.

IV. Mr. Schober's Harms were Caused by the Defendants' Actions.

59. Benedict and/or Oliver intentionally developed the Malware for the purpose of stealing cryptocurrency.

60. In or about October 2017—just days before the Malware appeared online—Benedict sent a message to the Bitcoin Developer's online mailing list describing the method used by the Malware to alter bitcoin addresses and steal bitcoins.[9]

61. Benedict's public GitHub software repositories webpage contains the powerful and sophisticated software programs deployed by the Malware.[10]

62. Benedict's GitHub repositories page includes a program designed for algorithmic trading at the Bitfinex cryptocurrency exchange, which is where, along with Mr. Schober's stolen funds, other victims' cryptocurrencies also stolen by the Malware were deposited on two separate occasions. [11]

---

[9] https://lists.linuxfoundation.org/pipermail/bitcoin-dev/2017-October/015211.html

[10] https://github.com/BenedictThompson-zz/

[11] The other thefts connected to the Malware occurred in or about November 2017.

63. Further, Benedict's Github repositories reveal that he copied and then independently developed the Electrum code (the source code necessary to deploy the Malware) just two weeks before Mr. Schober's cryptocurrency was stolen.

64. Exactly like the Malware, the code in Benedict's Github repositories contains software designed to monitor, generate, and interact with specific cryptocurrency (i.e., Bitcoin) wallet addresses.

65. But for Benedict and/or Oliver's creation of the Malware, Mr. Schober would not have had his privacy invaded, his computer damaged, and his cryptocurrency stolen.

66. Benedict and Oliver deliberately engaged in a scheme to publish false and misleading information that caused Mr. Schober to believe he was downloading non-malicious software affiliated with Electrum.

67. Benedict and/or Oliver (using one or more aliases) encouraged people to download the software on at least one public forum.

68. Additionally, Benedict and/or Read publicly represented that the software he or they posted on the public forum(s) was Electrum brand software and stated that the software did not contain malware.

69. But for Benedict and/or Oliver's false and misleading representations about the authenticity of the file Mr. Schober downloaded, Mr. Schober would not have had his privacy invaded, his computer damaged, and his cryptocurrency stolen.

70. Benedict and/or Oliver utilized the Malware to intercept and alter Mr. Schober's communications between his computer and the Bitcoin blockchain.

71. But for the interception and alteration of Mr. Schober's communications—specifically, the alteration of the clipboard function of Mr. Schober's computer—Mr. Schober would not have had his cryptocurrency stolen.

72. Benedict's Twitter account contains three tweets made during the weeks surrounding these thefts that indicate he used the Bitfinex exchange and had knowledge of how the Malware worked.

73. The IP address used by Benedict matches the IP address logged by the Bitfinex account responsible for receiving Mr. Schober's cryptocurrency.

CLAIMS FOR RELIEF

First Cause of Action
Conversion
(All Defendants)

74. The allegations in paragraphs 1 through 73 of this Complaint are repeated and realleged as if fully set forth herein.

75. By the actions described in this Complaint, Defendants converted Mr. Schober's personal property.

76. Mr. Schober owned and possessed the private keys proving his ownership and possession of property in the form of 16.4552 bitcoins (his "cryptocurrency").

77. The cryptocurrency taken by the Defendants from Mr. Schober is valuable.

78. The Defendants were not authorized to obtain, retain, or exercise control, dominion, or ownership over Mr. Schober's cryptocurrency.

79. The Defendants knowingly obtained, retained, and exercised control, dominion, or ownership over Mr. Schober's cryptocurrency, to the exclusion of Mr. Schober.

80. The Defendants specifically intended to permanently deprive Mr. Schober of his cryptocurrency.

81. By their refusal to respond to Mr. Schober's demand for the return of his cryptocurrency, the Defendants have refused to return Mr. Schober's cryptocurrency.

82. Mr. Schober has been deprived of the possession and use of his cryptocurrency for three years.

83. Mr. Schober suffered actual injury and damages of compensable value stemming from the converted cryptocurrency.

Second Cause of Action
Trespass to Chattel
(All Defendants)

84. The allegations in paragraphs 1 through 83 of this Complaint are repeated and realleged as if fully set forth herein.

85. By the actions described in this complaint, Benedict and Oliver committed common law trespass to chattel.

86. Mr. Schober's computer was at all relevant times in his possession.

87. Benedict and Oliver intentionally interfered with the physical condition of Mr. Schober's computer, and his possession of it.

88. Benedict and Oliver intentionally interfered with the physical condition of Mr. Schober's cryptocurrency wallet, and his possession of cryptocurrency.

89. Mr. Schober has been deprived of the use of his computer for more than two years.

90. Mr. Schober has been deprived of the use of cryptocurrency for more than three years.

Third Cause of Action
Civil Conspiracy
(All Defendant)

91. The allegations in paragraphs 1 through 90 of this Complaint are repeated and realleged as if fully set forth herein.

92. Benedict and Oliver conspired to develop and deploy and/or utilize the Malware to deprive Mr. Schober of his cryptocurrency.

93. Benedict and Oliver had a meeting of the minds on the object to be achieved and/or the course of action for accomplishing the development, deployment, and/or utilization of the Malware and/or the resulting theft.

94. Developing and deploying and/or utilizing the Malware is an overt act that is unlawful under the Computer Fraud and Abuse Act ("CFAA"), 18 U.S.C. § 1030.

95. Stealing cryptocurrency is an overt act that is unlawful according to common law and Colorado statutory law.

96. Mr. Schober incurred damages as a proximate result of Benedict and Oliver's conspiracy to develop and deploy the Malware and/or steal Mr. Schober's cryptocurrency.

Fourth Cause of Action
Violation of the Computer Fraud and Abuse Act, 18 U.S.C. § 1030
(All Defendants)

97. The allegations in paragraphs 1 through 96 of this Complaint are repeated and realleged as if fully set forth herein.

98. By the actions alleged in this Complaint, Benedict and Oliver violated the CFAA, 18 U.S.C. §§ 1030(a)(4), 1030(a)(5)(A), 1030(a)(5)(B), 1030(a)(5)(C), and 1030(g).

99. Mr. Schober's computer can connect to the Internet.

100. Benedict and/or Oliver intentionally accessed Mr. Schober's computer using the Malware, without Mr. Schober's authorization, to effect the theft of Mr. Schober's cryptocurrency.

101. Benedict and/or Oliver took these actions knowing that they would cause damage to Mr. Schober's computer, as well as damage to the information located on his computer.

102. Benedict and/or Oliver caused Mr. Schober's computer and much of the data on it to be unusable to him.

103. Because of Benedict and/or Oliver's actions, Mr. Schober suffered damage to his computer and damage to information on his computer, including being unable to access information and data on his computer and being unable to access his personal financial (i.e., cryptocurrency) account.

104. Mr. Schober spent in excess of $10,000 investigating who accessed his computer and damaged information on it.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff Andrew Schober requests that judgment be entered against Defendants and that the Court grant the following:

A. Judgment against Defendants for Plaintiff's asserted causes of action;

B. Pre- and post-judgment interest, as allowed by law;

C. An award of monetary damages, including punitive damages, as allowed by law;

D. Reasonable attorneys' fees and costs reasonably incurred, including but not limited to attorneys' fees and costs pursuant to 47 U.S.C. § 206; and

E. Any and all other and further relief to which Plaintiff may be entitled.

DEMAND FOR JURY TRIAL

Plaintiff demands a trial by jury of all issues so triable.

Dated: May 20, 2021

ANDERSON KILL, P.C.

By: /s/ Stephen Palley

Stephen Palley
Samuel Ballard

1717 Pennsylvania Avenue NW
Suite 200
Washington, DC 20006
Telephone: (202) 416-6500
Fax: (202) 416-6555
spalley@andersonkill.com
sballard@andersonkill.com

Attorneys for Plaintiff Andrew Schober