PIERCE BAINBRIDGE BECK PRICE & HECHT LLP
Thomas D. Warren (State Bar No. 160921)
twarren@piercebainbridge.com
Andrew Calderón (State Bar No. 316673)
acalderon@piercebainbridge.com
355 S. Grand Avenue, 44th Floor
Los Angeles, CA 90071
Telephone: (213) 262-9333
Facsimile: (213) 279-2008

Dwayne D. Sam (*pro hac application forthcoming*)
dsam@piercebainbridge.com
600 Pennsylvania Avenue NW
South Tower, Suite 700
Washington, DC 20004
Telephone: (202) 843-8342
Facsimile: (646) 968-4125

Counsel for Plaintiff Seth Shapiro

THE UNITED STATES DISTRICT COURT
FOR THE CENTRAL DISTRICT OF CALIFORNIA

SETH SHAPIRO,

Plaintiff,

v.

AT&T MOBILITY, LLC,

Defendant.

Case No. 2:19-cv-8972

CIVIL COMPLAINT

DEMAND FOR JURY TRIAL

I. NATURE OF THE ACTION

1. This action arises out of AT&T's repeated failure to protect its wireless cell service subscriber—Seth Shapiro—from its own employees, resulting in massive and ongoing violations of Mr. Shapiro's privacy, the compromise of his highly sensitive personal and financial information, and the theft of more than $1.8 million.

2. AT&T is the country's largest wireless service provider. Tens of millions of subscribers entrust AT&T with access to their confidential information, including information that can serve as a key to unlock subscribers' highly sensitive personal and financial information.

3. Recognizing the harms that arise when wireless subscribers' personal information is accessed, disclosed, or used without their consent, federal and state laws require AT&T to protect this sensitive information.

4. AT&T also recognizes the sensitivity of this data, and promises its subscribers that it "will protect [customers'] privacy and keep [their] personal information safe" and that it "will not sell [customers'] personal information to anyone, for any purpose. Period." AT&T repeatedly broke these promises.

5. In an egregious violation of the law and its own promises, and despite advertising itself as a leader in technological development and as a cyber security-savvy company, AT&T repeatedly failed to protect Mr. Shapiro's account and the sensitive data it contained. AT&T failed to implement sufficient data security systems and procedures and failed to supervise its own personnel, instead standing by as its employees used their position at the company to gain unauthorized access to Mr. Shapiro's account in order to rob, extort, and threaten him in exchange for money.

6. AT&T's actions and conduct were a substantial factor in causing significant financial and emotional harm to Mr. Shapiro and his family. But for

AT&T employees' involvement in a conspiracy to rob Mr. Shapiro, and AT&T's failure to protect Mr. Shapiro from such harm through adequate security and oversight systems and procedures, Mr. Shapiro would not have had his personal privacy repeatedly violated and would not have been a victim of SIM swap theft.

7. Mr. Shapiro brings this action to hold AT&T accountable for its violations of federal and state law, and to recover for the grave financial and personal harm suffered by Mr. Shapiro and his family as a direct result of AT&T's acts and omissions, as detailed herein.

II. THE PARTIES

8. Plaintiff Seth Shapiro is, and at all relevant times was, a resident of California. Mr. Shapiro currently resides in Torrance, CA, with his wife and two young children.

9. Mr. Shapiro is a two-time Emmy Award-winning media and technology expert, author, and adjunct professor at the University of Southern California School of Cinematic Arts. He regularly advises Fortune 500 companies on business development in media and technology. Mr. Shapiro was also an early investor in digital currencies.

10. Mr. Shapiro is a former AT&T wireless customer. He purchased a wireless cell phone plan from AT&T in Los Angeles, California in approximately 2006 for personal use and was an active, paying AT&T wireless subscriber at all times relevant to the allegations in this Complaint.

11. Defendant AT&T Mobility, LLC (hereinafter, "AT&T") is a Delaware limited liability corporation with its principal office or place of business in Brookhaven, Georgia. AT&T "provides nationwide wireless services to consumers and wholesale and resale wireless subscribers located in the United States or U.S. territories" and transacts or has transacted business in this District and throughout the United States. It is the second largest wireless carrier in the United States, with

more than 153 million subscribers, earning $71 billion in total operating revenues in 2017 and $71 billion in 2018. As of December 2017, AT&T had 1,470 retail locations in California.[1]

12. AT&T provides wireless service to subscribers in the United States. AT&T is a "common carrier" governed by the Federal Communications Act ("FCA"), 47 U.S.C. § 151 *et seq.* AT&T is regulated by the Federal Communications Commission ("FCC") for its acts and practices, including those occurring in this District.

13. AT&T Inc., AT&T's parent company, acknowledged in its 2018 Annual Report that its "profits and cash flow are largely driven by [its] Mobility business" and "nearly half of [the] company's EBITDA (earnings before interest, taxes, depreciation and amortization) come from Mobility."[2]

14. Despite the importance of its mobility business, instead of focusing on providing ramping up security for their customers, AT&T Inc. has gone on a buying spree costing over $150 billion, acquiring: Bell South (including Cingular Wireless and Yellowpages.com), Dobson Communications, Edge Wireless, Cellular One, Centennial, Wayport, Qualcomm Spectrum, Leap Wireless, DirecTV, and Iusacell and NII Holdings (now AT&T Mexico). During the same period, AT&T's mobile phone business was rated as the worst among major providers. Consumer Reports named it the "worst carrier" in 2010, and the next year, J.D. Power found AT&T's network the least reliable in the country—a dubious achievement that it also earned in prior years. Little wonder that its customers were the least happy of subscribers of the Big Four carriers according to the American Consumer Index. In the meantime, AT&T Inc. has purchased for a total equity value of $85.4 billion Time Warner Inc.—the owner of HBO, Warner Bros,

[1] "About Us," AT&T, *available at* https://engage.att.com/california/about-us/. All URLs in this complaint were last accessed on October 15, 2019.
[2] *Id.*

CNN, Turner Broadcasting, Cartoon Network, Turner Classic Movies, TBS, TNT and Turner Sports.

III. JURISDICTION AND VENUE

15. This Court has jurisdiction over this matter under 28 U.S.C. § 1331 because this case arises under federal question jurisdiction under the Federal Communications Act ("FCA"). 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. The Court also has jurisdiction over this action pursuant to 28 U.S.C. § 1332 because Mr. Shapiro is a citizen of a different state than AT&T.

16. This Court has personal jurisdiction over AT&T because AT&T purposefully directs its conduct at California, transacts substantial business in California (including in this District), has substantial aggregate contacts with California (including in this District), engaged and is engaging in conduct that has and had a direct, substantial, reasonably foreseeable, and intended effect of causing injury to persons in California (including in this District), and purposely avails itself of the laws of California. AT&T had more than 33,000 employees in California as of 2017, and 1,470 retail locations in the state.[3] Mr. Shapiro purchased his AT&T wireless plan in California, visited AT&T retail locations in California, and was injured in California by the acts and omissions alleged herein.

17. In accordance with 28 U.S.C. § 1391, venue is proper in this District because a substantial part of the conduct giving rise to Mr. Shapiro's claims occurred in this District and Defendant transacts business in this District. Mr. Shapiro purchased his AT&T wireless plan in this District and was harmed in this District, where he resides, by AT&T's acts and omissions, as detailed herein.

IV. ALLEGATIONS APPLICABLE TO ALL COUNTS

[3] "About Us," AT&T California, *supra* at 1.

18. As a telecommunications carrier, AT&T is entrusted with the sensitive wireless account information and personal data of millions of Americans, including Mr. Shapiro's confidential and sensitive personal and account information.

19. Despite its representations to its customers and its obligations under the law, AT&T has failed to protect Mr. Shapiro's confidential information. On at least four occasions between May 16, 2018 and May 18, 2019, AT&T employees obtained unauthorized access to Mr. Shapiro's AT&T wireless account, viewed his confidential and proprietary personal information, and transferred control over Mr. Shapiro's AT&T wireless number from Mr. Shapiro's phone to a phone controlled by third-party hackers in exchange for money. The hackers then utilized their control over Mr. Shapiro's AT&T wireless number—including control secured through cooperation with AT&T employees—to access his personal and digital finance accounts and steal more than $1.8 million from Mr. Shapiro.

20. This type of telecommunications account hacking behavior is known as "SIM swapping."

A. SIM Swapping is a Type of Identity Theft Involving the Transfer of a Mobile Phone Number.

21. On four occasions in 2018 and 2019, Mr. Shapiro was the target of "SIM swapping."

22. "SIM swapping" refers to a relatively simple scheme, wherein third parties take control of a victim's wireless phone number. The hackers then use that phone number as a key to access the victim's digital accounts, such as email, file storage, and financial accounts.

23. Most cell phones, including the iPhone owned by Mr. Shapiro at the time of his SIM swaps, have internal SIM ("subscriber identity module") cards. A SIM card is a small, removable chip that allows a cell phone to communicate with the wireless carrier and the carrier to know what subscriber account is associated with that phone. The connection between the phone and the SIM card is made

through the carrier, which associates each SIM card with the physical phone's IMEI ("international mobile equipment identity"), which is akin to the phone's serial number. Without a working SIM card and effective SIM connection, a phone typically cannot send or receive calls or text messages over the carrier network. SIM cards can also store a limited amount of account data, including contacts, text messages, and carrier information, and that data can help identify the subscriber.

24. The SIM card associated with a wireless phone can be changed. If a carrier customer buys a new phone that requires a different sized SIM card, for example, the customer can associate his or her account with a new SIM card and the new phone's IMEI by working with their cell phone carrier to effectuate the change. This allows carrier customers to move their wireless number from one cell phone to another and to continue accessing the carrier network when they switch cell phones. For a SIM card change to be effective, the carrier must authenticate the request and actualize the change. AT&T allows its employees to conduct SIM card changes for its customers remotely or in its retail stores.

25. A SIM swap refers to an unauthorized and illegitimate SIM card change. During a SIM swap attack, the SIM card associated with the victim's wireless account is switched from the victim's phone to a phone controlled by a third party. This effectively moves the victim's wireless phone—including any incoming data, texts, and phone calls associated with the victim's phone—from their phone to a phone controlled by the third party (also referred to herein as a "hacker"). The hacker's phone then becomes the phone associated with the victim's carrier account, and the hacker receives all of the text messages and phone calls intended for the victim.[4] Meanwhile, the victim's phone loses its connection to the carrier network.

[4] As described by federal authorities in prosecuting SIM swap cases, SIM swapping enables hackers to "gain control of a victim's mobile phone number by linking that number to a subscriber identity module ('SIM') card controlled by [the hackers]—resulting in the victim's

26. Once hackers have control over the victim's phone number, they can use that control to access the victim's personal online accounts, such as email and banking accounts, through exploiting password reset links sent via text message to the now-hacker-controlled-phone or the two-factor authentication processes associated with the victim's digital accounts. Two-factor authentication allows digital accounts to be accessed without a password, or allows the account password to be changed. One common form of two-factor authentication is through text messaging. Rather than enter a password, the hacker requests that a password reset be sent to the mobile phone number associated with the account. Because the hacker now controls that phone number, the reset code is sent to them. The hacker can then log into, and change the password for, the victim's account, allowing them to access the contents of the account.[5]

27. The involvement of a SIM swap victim's wireless carrier is critical to an effective SIM swap. In order for a SIM swap to occur and for a SIM swap victim to be at any risk, the carrier must receive a request to change a victim's SIM card and effectuate the transfer of the victim's phone number from one SIM card to another.

28. In Mr. Shapiro's case, not only did AT&T employees access his account and authorize changes to that account without Mr. Shapiro's consent, but its employees actively *profited* from this unauthorized access by knowingly giving control over his phone number to hackers for the purposes of robbing him.

---

phone calls and short message service ('SMS') messages being routed to a device controlled by [a hacker]." *United States of America v. Conor Freeman, et al.*, No. 2:19-cr-20246-DPH-APP (E.D. Mich. Filed Apr. 18, 2019) (hereafter, "Freeman Indictment"), ECF. No. 1 at ¶ 3 (attached hereto as Exhibit A).

[5] *See, e.g.*, *Id.* at ¶ 4 ("Once [hackers] had control of a victim's phone number, it was leveraged as a gateway to gain control of online accounts such as the victim's email, cloud storage, and cryptocurrency exchange accounts. Sometimes this was achieved by requesting a password-reset link be sent via [text messaging] to the device control by [hackers]. Sometimes passwords were compromised by other means, and [the hacker's] device was used to received two-factor authentication ('2FA') message sent via [text message] intended for the victim.").

B. AT&T Allowed Unauthorized Access to Mr. Shapiro's Account Four Times Over the Course of Approximately One Year.

29. Between May 16, 2018 and May 18, 2019, AT&T employees accessed Mr. Shapiro's AT&T wireless account without his authorization, obtained his confidential and proprietary personal information, and sold that information to third parties who then used it to steal from Mr. Shapiro, access his sensitive and confidential information, and threaten his family.

30. On May 16, 2018 at approximately 1:35 PM ET, Mr. Shapiro's AT&T SIM card was changed without his knowledge or authorization for the first time.

31. At the time of the SIM swap, Mr. Shapiro was attending a conference in New York City. He noticed that his AT&T cell phone had lost service. Mr. Shapiro's device was no longer connected to the AT&T wireless network, and he was no longer able to place or receive wireless calls.

32. Mr. Shapiro immediately suspected that a SIM swap attack was underway and called AT&T in an attempt to secure his account. Mr. Shapiro informed the AT&T customer service agent that he suspected his account had been accessed without authorization and that he was in possession of large amounts of digital currency, which he feared could be at risk.

33. During his call with AT&T, Mr. Shapiro repeatedly asked to speak to upper management or to be connected to the AT&T department responsible for security. AT&T records confirm Mr. Shapiro's request to speak to the fraud department. Mr. Shapiro was (incorrectly) told that no such department existed, and his call was never escalated to management. Instead, he was put on lengthy holds and ultimately told to turn off his phone and go to an AT&T retail location for further assistance. His AT&T service was then suspended.

34. Immediately upon ending the call with AT&T's customer service, Mr. Shapiro went to an AT&T retail store in Manhattan, New York.[6] Upon arriving,

[6] This AT&T retail store is located at 1330 Avenue of the Americas, New York, NY 10019.

Mr. Shapiro informed AT&T employees—including an AT&T sales representative, Juneice Arias—that he suspected unauthorized SIM swap activity on his account and once again advised that he had confidential information and digital currency that could be at risk.

35. AT&T employees advised Mr. Shapiro to purchase a new wireless phone with a new SIM card from AT&T. On this advice, Mr. Shapiro purchased a new iPhone for several hundred dollars, as well as a new SIM card, in the AT&T retail store. AT&T employees then activated the new phone and the new SIM card and restored Mr. Shapiro's service, thereby allowing Mr. Shapiro to regain control over his AT&T cell phone number.

36. AT&T employees told Mr. Shapiro at that time that they had noted the SIM swap activity in his account and assured him that his SIM card would not be swapped again without his authorization. On this assurance, Mr. Shapiro decided not to close his AT&T account.

37. Mere minutes later—while Mr. Shapiro was still in the AT&T retail store—Mr. Shapiro's AT&T account was again improperly accessed, and the SIM card associated with his phone number was changed. Mr. Shapiro again lost control over his AT&T cell phone number.

38. Mr. Shapiro immediately informed AT&T employees that AT&T had once again allowed an unauthorized SIM swap. Employees informed him that he needed to wait until it was his turn to be assisted.

39. Mr. Shapiro waited for approximately 45 minutes inside the AT&T retail store for help from AT&T employees. In that time, third-party individuals were able to use their control over Mr. Shapiro's AT&T cell phone number to access Mr. Shapiro's personal and financial accounts and rob him of approximately $1.8 million, all while Mr. Shapiro stood helplessly in the AT&T store asking for the company's help.

40. While third parties had control over Mr. Shapiro's AT&T wireless number, they used that control to access and reset the passwords for Mr. Shapiro's accounts on cryptocurrency exchange platforms, including KuCoin, Bittrex, Wax, Coinbase, Huobi, Crytopia, LiveCoin, HitBTC, Coss.io, Liqui, and Bitfinex. Cryptocurrency exchanges are online platforms where different forms of cryptocurrency (e.g. bitcoin) are bought and sold.

41. Before the May 2018 SIM swaps, Mr. Shapiro had raised funds in the form of cryptocurrency for a new business venture. This capital, as well as Mr. Shapiro's personal funds, was accessed by the hackers utilizing their control over Mr. Shapiro's AT&T wireless number, although the business funds were stored separately from Mr. Shapiro's personal funds.

42. By utilizing their control over Mr. Shapiro's AT&T cell phone number—and the control of additional accounts (such as his email) secured through that number by utilizing two factor authentication—these third-party hackers were able to access Mr. Shapiro's accounts on various cryptocurrency exchange platforms, including the accounts he controlled on behalf of his business venture. The hackers then transferred Mr. Shapiro's currency from Mr. Shapiro's accounts into accounts that they controlled.[7] In all, they stole more than $1.8 million from Mr. Shapiro in the two consecutive SIM swap attacks on May 16, 2018.

43. On information and belief, the hackers also utilized their control over Mr. Shapiro's AT&T wireless number to access and steal Mr. Shapiro's currency

[7] *See* Affidavit for Search Warrant, *Florida v. Ricky Handschumacher*, No. 18-cf-4271-AXWS (6th Dis. Fl. July 25, 2018) (attached hereto as Exhibit B) at p. 8 (explaining how hackers—including hackers involved in robbing Mr. Shapiro—would "gain access to the victim's email accounts and cryptocurrency exchanges…[and] use the victim's funds to purchase cryptocurrencies and transfer it to a accounts [sic] or wallets the [hackers] controlled."). Due to the nature of cryptocurrency, this process makes it extremely difficult to track and seize the location of stolen cryptocurrency.

on cryptocurrency exchanges (including Liqui.io, Livecoin, and Huobi) to which Mr. Shapiro was never able to regain access.

44. The hackers also used their control over Mr. Shapiro's AT&T cell phone number to access and change the passwords for approximately 15 of Mr. Shapiro's online accounts, including four email addresses, his Evernote account (a web application for taking notes and making task lists), and his PayPal account (a digital payment platform).

45. It took Mr. Shapiro approximately 14 hours to regain access to and restore control over his email and other personal accounts. By then, however, the damages was done: these accounts, and all of their contents, had already been compromised.

46. Criminal investigations into the May 2018 breaches to Mr. Shapiro's AT&T account and the resulting theft revealed that at least two AT&T employees, acting in the scope of their employment, accessed and permitted others to access Mr. Shapiro's AT&T account and the confidential information contained therein.[8] As federal authorities describe, "These employees, while not necessarily knowing the entirety of [the hackers] plans, were aware that they were assisting in the theft of identities of subscribers to their employer's services."[9]

47. The two AT&T employees involved, Robert Jack and Jarratt White,[10] reside in Arizona. AT&T confirmed their employment,[11] their involvement in the

[8] *See* Criminal Complaint and Affidavit, *United States of America v. Jarratt White, et al.*, No. 2:19-mj-30227-DUTY (E.D. Mich. Filed May 2, 2019) (hereafter, "White Affidavit"), ECF No. 1 (attached hereto as Exhibit C).
[9] *Id.* at ¶ 8.
[10] *Id.* at ¶¶ 10-15 (describing White's involvement in the unauthorized access of Mr. Shapiro's AT&T account and the resulting theft) and ¶¶ 16-19 (describing Jack's involvement).
[11] *Id.* at ¶ 15 ("AT&T confirmed that WHITE was a contract employee from Tucson, Arizona.") and ¶ 16 ("Based on records provided from AT&T, ROBERT JACK, a second AT&T contract employee from Tucson, Arizona… .")

unauthorized access of Mr. Shapiro's account,[12] and their involvement in the two SIM swaps that occurred on May 16, 2018.

48. Specifically, criminal investigations reveal that a third-party (an individual identified by authorities as "JD") paid Jack and White to change the SIM card associated with Mr. Shapiro's AT&T account from the SIM card in Mr. Shapiro's phone to a SIM card in a phone controlled by JD and others.[13]

49. In order to effectuate the swaps, Jack and/or White used their access to Mr. Shapiro's account—access gained through their AT&T employment—to view his confidential AT&T account information and effectuate the SIM swaps without Mr. Shapiro's knowledge or consent.

50. JD paid White $4,300 in exchange for White using his position, knowledge, and authority as an AT&T employee to conduct SIM swaps, including the May 16, 2018 SIM swaps of Mr. Shapiro.[14] White then paid Jack $585.25 for his involvement in the swaps.[15]

51. On information and belief, AT&T data shows that White and Jack were prolific SIM swappers. White conducted 29 *unauthorized SIM swaps* in May 2018,[16] while Jack conducted *12 unauthorized swaps* that same month.[17]

52. Criminal investigations have also identified the AT&T employees' third-party co-conspirators and revealed additional information about the employees' involvements in the scheme.

53. For example, police officers located documents on the computer of one co-conspirator hacker (identified as "CS1") labeled "ATT Plug."[18] In the SIM

[12] *Id.* at ¶¶ 11, 15-16.
[13] *Id.* at ¶¶ 11, 16-19.
[14] *Id.* at ¶¶ 11-12.
[15] *Id.* at ¶ 19.
[16] *Id.* at ¶ 15.
[17] *Id.* at ¶ 16.
[18] Ex. B at p. 7.

swap context, a "plug" is a telecommunication carrier employee who uses their knowledge and access to assist in SIM swaps.

54. Investigators were also able to obtain a log of a chat conversation held online between the third-party co-conspirator hackers, wherein they plotted and executed the theft of Mr. Shapiro's currency.[19]

55. The chat begins with the group discussing working with an AT&T employee to access Mr. Shapiro's AT&T wireless account and swap his SIM card. At 1:19 PM on May 16, 2018, one member of the group asks, "What is plug doing[?]"[20] On information and belief, this refers to the group's AT&T plug: White or Jack. The same member requests at 1:31 that another member "message [the plug] and tell him hurry up[.]"[21]

56. Beginning at 1:38, a member informs the group that the plug is "doing it [right now]" and then: "It's activated."[22] On information and belief, this refers to Mr. Shapiro's AT&T account being activated on a phone utilized by the hackers – the result of a successful SIM swap effectuated by one or more of the involved AT&T employees.

57. Once the SIM swap was complete, the group began using their control over Mr. Shapiro's AT&T wireless number to access his personal and financial accounts. At 1:58 and 2:10 PM, the chat log shows the group using Mr. Shapiro's number (which they share over the chat) to access and reset the passwords for his email accounts.[23]

58. At 2:18 PM, the chat log shows the group accessing Mr. Shapiro's Bittrex account and withdrawing his digital currency.[24]

---

[19] *Id.* at Attachment A.
[20] *Id.* at Attachment A, pg. 1.
[21] *Id.* at Attachment A, pg. 2.
[22] *Id.* at Attachment A, pgs. 2-5.
[23] *Id.* at Attachment A, pgs. 5-6
[24] *Id.* at Attachment A, pg. 6.

59. The individuals would not have been able to access these accounts but for their utilization of Mr. Shapiro's cell phone number, control of which was obtained through the use of AT&T's employees and systems.

60. Throughout the chat, the group refers to an additional male individual—the AT&T plug—helping them access Mr. Shapiro's account. At 3:11 PM, one member brags, "*my ATT (AT&T) guy… Is a supervisor… He ain't ever getting fired.*"[25]

61. The chat also reflects Mr. Shapiro's attempt to regain control of his AT&T account. At 3:39, one member warns that Mr. Shapiro is "trying to get number back."[26] Another—referring to the AT&T co-conspirator—ask whether he wants "[his] guy to swap it back?"[27] At the end of the chat, a group member brags that they "made 1.3 [million]" and they begin plotting about how to route the stolen cryptocurrency through various accounts and currencies in order to cover their trail.[28] They also brag about plans to "buy some Gucci" or a "dream car" with the money they stole from Mr. Shapiro.[29]

62. As these hackers and AT&T employees stole Mr. Shapiro's life savings and made plans to spend it on luxury goods, Mr. Shapiro was still standing in the AT&T retail store in Manhattan, NY, asking AT&T for help. He was told to wait as his accounts were drained and his personal information compromised.

63. After the May 2018 SIM swaps, AT&T employees told Mr. Shapiro that his account would be safe from future attacks because they had put a note on his account that would prevent any future SIM swaps.

[25] *Id*. at Attachment A, pg. 7 (emphasis added).
[26] *Id.* at Attachment A. pg. 8.
[27] *Id.*
[28] *Id.* at Attachment A. pg. 10.
[29] *Id.* at Attachment A. pg. 9.

64. Mr. Shapiro also changed his AT&T account passcodes on the advice of AT&T employees. AT&T informs its customers that these account passcodes—which are different than account sign-in passwords or the passcodes used to access a wireless device—are used to protect their wireless accounts and may be required when a customer manages their AT&T account online or in an AT&T store.[30] AT&T employees represented to Mr. Shapiro that this passcode would not be shared with anyone, and would protect his account from future unauthorized SIM swaps. Mr. Shapiro decided not to close his AT&T account in reliance on these assurances.

65. Mr. Shapiro's trust in AT&T was misplaced. On November 1, 2018, Mr. Shapiro again noticed that his cell phone had lost service, and suspected a SIM swap. Shortly thereafter, he received an alert that someone had accessed and changed the password to—at minimum—his Google email accounts. This also caused all information stored in this account—including sensitive and confidential personal, financial, and legal information—to be compromised.

66. Mr. Shapiro contacted AT&T and confirmed that he had indeed been SIM swapped a third time. Again, AT&T employees represented to Mr. Shapiro that they had taken steps to prevent any further SIM swaps on his account.

67. On May 14, 2019, Mr. Shapiro received a letter from AT&T's Director of Compliance, Nena M. Romano, informing him that "an employee of one of [AT&T's] service providers accessed [Mr. Shapiro's] Customer Proprietary Network Information [CPNI] without authorization."[31] The letter did not indicate which of the three prior SIM swap attacks it concerned. It stated that AT&T had "taken appropriate action" regarding the AT&T employee involved and had

[30] "Get info on passcodes for wireless accounts," AT&T, *available at* https://www.att.com/esupport/article.html#!/wireless/KM1049472?gsi=tp3wtr.
[31] Attached hereto as Exhibit D.

"notified federal law enforcement concerning the unauthorized access of your CPNI as required by Federal Communications Commission regulations."

68. Despite these assertions, Mr. Shapiro was SIM swapped for a *fourth* time on May 18, 2019, at approximately 10:45 PM. Again, Mr. Shapiro lost AT&T service and begun receiving alerts that the passwords for his personal digital accounts had been changed.

69. Mr. Shapiro immediately contacted AT&T customer service. After several long holds and Mr. Shapiro's repeated requests, his call was elevated to an AT&T supervisor. The supervisor, Marcus,[32] informed Mr. Shapiro that he had been SIM swapped again but refused to tell Mr. Shapiro who had authorized the swap.

70. Mr. Shapiro asked the supervisor why the secret passcode that AT&T had promised him would protect his account failed to provide that protection. The AT&T supervisor refused to provide an answer.

71. The supervisor then informed Mr. Shapiro that he would request that his AT&T account be transferred back to Mr. Shapiro's phone. He estimated this would take between 2 and 4 hours. Meanwhile—upon information and belief—hacker continued to have control over his AT&T wireless account throughout that time, and used that control to access his personal and financial accounts.

72. Mr. Shapiro repeatedly asked the supervisor to escalate his call to a higher authority at AT&T. Eventually, he was transferred to an AT&T manager, Tom. The manager informed him that in order to "reverse the unauthorized SIM card change," he would need to "file a ticket" to submit a reversal request—which "normally completes within 2 to 4 hours." He told Mr. Shapiro that he would sever the line in the meantime. It took the manager several minutes to "process" the ticket requesting a reversal. He then informed Mr. Shapiro that AT&T would send

[32] The AT&T employees with whom Mr. Shapiro spoke refused to provide their last names.

a pin code to another active line on his AT&T account to validate the reversal request. This required Mr. Shapiro to get his 12-year-old daughter out of bed, after midnight, to use her phone to receive the pin code. The manager told Mr. Shapiro they would "investigate" how his "account got compromised."

73. During this attack, Mr. Shapiro's Yahoo, Google, Windows, PayPal, Coinbase, and Evernote accounts—at minimum—were accessed and their contents compromised. The hacker changed the passwords on his Evernote, PayPal, Coinbase, and G-mail accounts (temporarily locking Mr. Shapiro out of the accounts), changed the recovery email for his G-mail account to an email they controlled, and deleted his G-mail security question. This also caused all information stored in these accounts—including sensitive and confidential person, financial, and legal information—to be compromised.

74. On July 19, 2019, Mr. Shapiro received another letter from AT&T's Director of Compliance, Nena M. Romano, informing him that, once again, "an employee of one of [AT&T's] service providers accessed [Mr. Shapiro's] Customer Proprietary Network Information (CPNI) without authorization."[33] The letter did not indicate which of the four SIM swap attacks it concerned. It stated that AT&T had "taken appropriate action" regarding the AT&T employee involved and had "notified federal law enforcement concerning the unauthorized access of your CPNI as required by Federal Communications Commission regulations."

75. On September 6, 2019, Mr. Shapiro received a third letter from Ms. Romano, informing him that "an unknown and unauthorized person gained access to [Mr. Shapiro's] Customer Proprietary Network Information (CPNI) without authorization."[34] Once again, the letter did not indicate which of the four SIM swap attacks it concerned. It stated that AT&T had "moved quickly to disable system access to the unauthorized person" and had "notified federal law enforcement

[33] Attached hereto as Exhibit E.
[34] Attached hereto as Exhibit F.

concerning the unauthorized access of your CPNI as required by Federal Communications Commission regulations."

76. The SIM swaps have exposed Mr. Shapiro and his family to ongoing threats of physical harm and extortion. On February 10, 2019, Mr. Shapiro received—on the same AT&T wireless line that had been hacked—text message threats from an anonymous individual (set forth below in Figure 1).

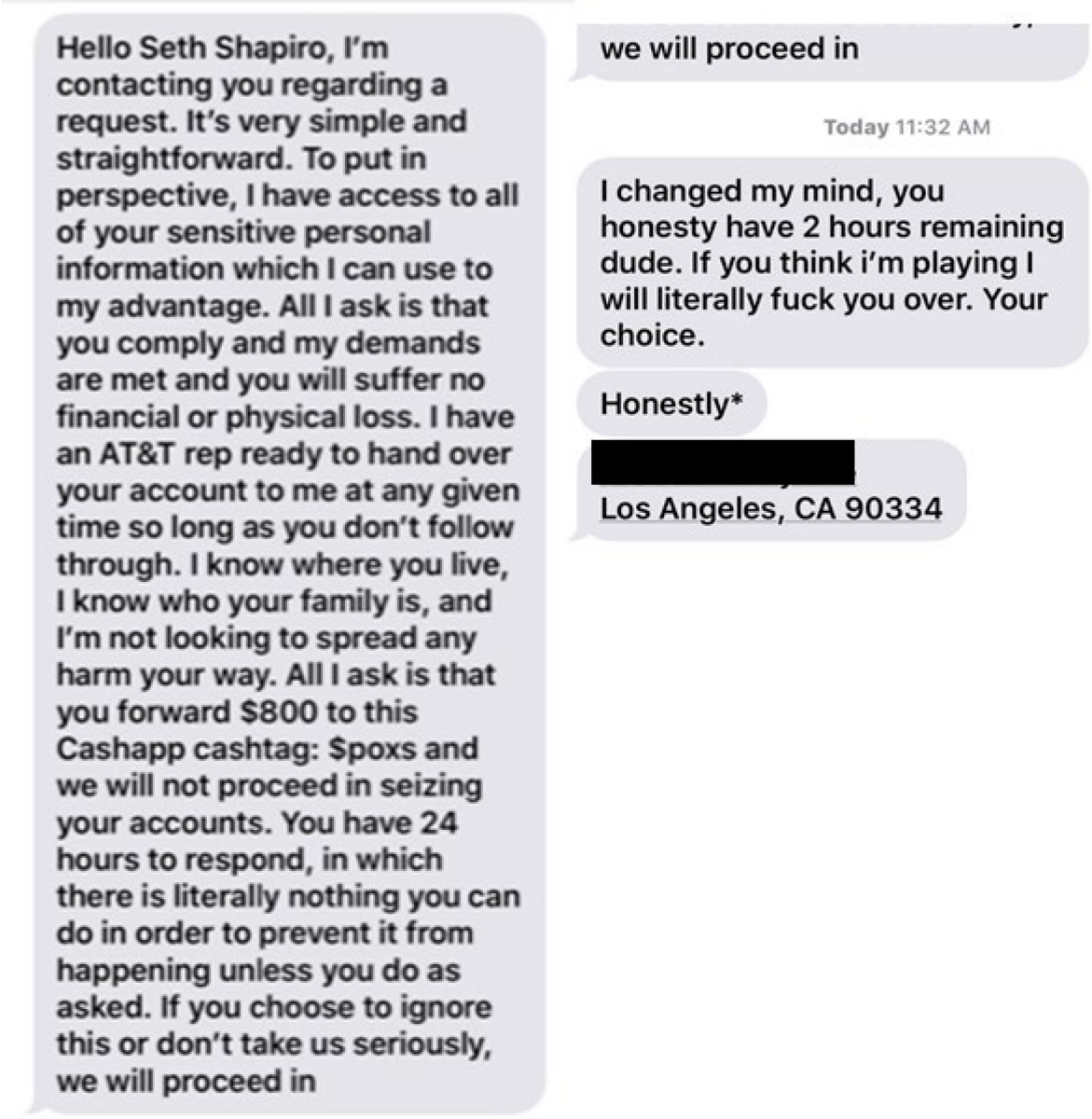


Figure 1

77. This individual knew Mr. Shapiro's name and AT&T wireless number and warned that they had "access to all of [his] sensitive personal information[.]" The harasser also threatened an additional SIM swap and informed Mr. Shapiro that they *still had access to AT&T employees who would aid them in further harm against Mr. Shapiro*. Specifically, they warned that they had "*an AT&T rep ready to hand over [Mr. Shapiro's] account to [them] at any given time[.]*" They warned that they knew where Mr. Shapiro and his family lived—and sent his exact current address (redacted below)—and demanded $800 to prevent harm to Mr. Shapiro and his family.

78. After Mr. Shapiro received these threats, a sergeant at the Santa Clara County Sherriff's Office informed Mr. Shapiro that he had personally contacted AT&T to inform them of the threats and requested that they monitor Mr. Shapiro's accounts. Despite this warning, Mr. Shapiro's account was authorized without his consent, and his SIM card swapped, approximately 3 months later.

79. The financial and personal lives of Mr. Shapiro and his family have been devastated as a result of AT&T's failure to safeguard Mr. Shapiro's account.

80. As a result of the May 2018 hacks detailed above, Mr. Shapiro lost more than $1.8 million in digital currency. This money constituted the entirety of the profits from the sale of Mr. Shapiro's family home and his life savings. As a result of the loss of that money, Mr. Shapiro and his family have not had the finances to buy another home, causing feelings of instability and anxiety for the whole family.

81. The financial strain resulting from the robbery of Mr. Shapiro has caused extreme anxiety and distress for Mr. Shapiro and his family.

82. Mr. Shapiro's wife, who previously took full time care for their young child, has had to return to work due to the financial strain and pressure. As a

consequence of the SIM swap attacks, she has suffered from anxiety, emotional distress, and loss of sleep and has had less time to see to the needs of her children.

83. Mr. Shapiro's two children have also suffered. Mr. Shapiro had to undertake the difficult task of explaining the theft to his four-year-old child, who now expresses fear of hackers and robbers and feelings of instability. The Shapiros also have a medically fragile child, who has suffered emotional distress as a result of the financial and emotional strain on the family. Both children require medical treatment as a result of the SIM swap attacks, and Mr. Shapiro has had to pay for that treatment out of pocket.

84. Mr. Shapiro has experienced immense harm as a result of the SIM swaps. He has suffered from anxiety, loss of sleep, and extreme depression. The emotional and financial consequences have also caused marital stress. Mr. Shapiro has had to seek extended professional medical help as a result.

85. The digital currency stolen during the SIM swap attacks also included cryptocurrency raised by Mr. Shapiro for a business venture. As a result of the theft, Mr. Shapiro had to end the venture and lay off all employees. He intends to repay each of the investors the amount they invested in the project which was stolen during the SIM swap attacks. He also suffered professional reputational damages when the venture ended, and investments were lost as a result of the theft.

86. Mr. Shapiro and his family's highly sensitive and confidential personal, legal, and business information have also been compromised as a result of the SIM swaps. This includes color copies of their passports, their social security numbers, their TSA numbers, password and log-in information for additional accounts, and confidential financial, business, and legal information. All of this information is now at a high risk of being posted or bought and sold on the dark web by criminals and identity thieves, putting Mr. Shapiro, his wife, and

two young children at ongoing risk of significant privacy violations, extortion, identity theft, and countless unknown harms.

C. AT&T's Repeated Failures to Protect Mr. Shapiro's Account from Unauthorized Access Are a Violation of Federal Law.

87. AT&T is the world's largest telecommunications company and provider of mobile telephone services. As a common carrier,[35] AT&T is governed by the Federal Communications Act of 1934, as amended ("FCA"),[36] and corresponding regulations passed by the FCC.[37]

88. Recognizing the sensitivity of data collected by cell carriers, Congress, through the FCA, requires AT&T to protect Mr. Shapiro's sensitive personal information to which it has access as a result of its unique position as a telecommunications carrier.[38]

89. Section 222 of the FCA, which became part of the Act in 1996, requires AT&T to protect the privacy and security of information about its customers. Likewise, Section 201(b) of the Act requires AT&T's practices related to the collection of information from its customers to be "just and reasonable" and declares unlawful any practice that is unjust or unreasonable.[39]

90. AT&T's most specific obligations to protect its customers concerns a specific type of information, called CPNI.[40] Specifically, the FCA "requires telecommunications carriers to take specific steps to ensure that CPNI is adequately protected from unauthorized disclosure."[41]

---

[35] 47 U.S. Code § 153(51).
[36] 47 U.S.C. § 151 *et seq.*
[37] 47 C.F.R. § 64.2001 *et seq.*
[38] 47 U.S.C. § 222.
[39] 47 U.S.C. § 201(b).
[40] 47 U.S.C. § 222(a).
[41] Report and Order and Further Notice of Proposed Rulemaking, *In the Matter of Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information*, 22 F.C.C. Rcd. 6927 ¶ 1 (April 2, 2007) (hereafter, "2007 CPNI Order").

91. Carriers such as AT&T are liable for failures to protect their customers unauthorized disclosures.[42] The FCC has also stated that "[t]o the extent that a carrier's failure to take reasonable precautions renders private customer information unprotected or results in disclosure of individually identifiable CPNI, . . . a violation of section 222 may have occurred."[43]

92. CPNI is defined as "information that relates to the quantity, technical configuration, type, destination, location, and amount of use of a telecommunications service subscribed to by any customer of a telecommunications carrier, and that is made available to the carrier by the customer solely by virtue of the carrier-customer relationship; and . . . information contained in the bills pertaining to telephone exchange service or telephone toll service received by a customer of a carrier."[44]

93. As AT&T admitted to Mr. Shapiro in its three letters,[45] his CPNI was breached by AT&T employees or "unknown and unauthorized person[s]" when they accessed his account and swapped his SIM card without authorization. In each letter, AT&T informed Mr. Shapiro that "an employee of one of [its] service providers accessed [his] Customer Proprietary Network Information (CPNI) without authorization."[46]

94. When employees accessed Mr. Shapiro's account, his CPNI was visible. On information and belief, this includes, but was not limited to, information about the configuration, type, and use of his subscribed AT&T services, his personal information, his SIM card details, and his billing

[42] 47 U.S.C. §§ 206, 207.
[43] Declaratory Ruling, *In the Matter of Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information & Other Customer Information*, 28 F.C.C. Rcd. 9609 ¶ 30 (2013) (hereafter, "2013 CPNI Order").
[44] 47 U.S.C. § 222(h)(1).
[45] *See.* Exs. D & E.
[46] *Id.*

information. AT&T employees then used this information to effectuate an unauthorized SIM swap.

95. This type of unauthorized use of Mr. Shapiro's CPNI is illegal under the FCA. The FCA forbids AT&T from "us[ing], disclos[ing], or permit[ting] access to" CPNI, except in limited circumstances.[47] As AT&T admitted in its May 2019 letter, this extends to the carrier's own employees.

96. AT&T may only use, disclose, or permit access Mr. Shapiro's CPNI: (1) as required by law; (2) with his approval; or (3) in its provision of the telecommunications service from which such information is derived, or services necessary to or used in the provision of such telecommunications service.[48] Beyond such use, "the Commission's rules require carriers to obtain a customer's knowing consent before using or disclosing CPNI."[49]

97. AT&T failed to protect Mr. Shapiro from authorized use of his CPNI. AT&T permitted its employees to use and/or disclose Mr. Shapiro's CPNI without obtaining Mr. Shapiro's knowing consent beforehand. AT&T employees, acting within the scope of their employment, likewise did not seek Mr. Shapiro's knowing consent before using, disclosing, and/or permitting access to his CPNI when they accessed his account and swapped his SIM card. Because such conduct does not fit within the FCA's recognized legitimate uses, it constitutes a violation of the FCA.

98. Pursuant to the FCA, the FCC has developed comprehensive rules concerning AT&T's obligations under its duty to protect customers' CPNI.[50] This

[47] 47 U.S.C. § 222(c)(1).
[48] 47 U.S.C. § 222.
[49] 2007 CPNI Order ¶ 8 (emphasis added).
[50] *See* 47 CFR § 64.2001("The purpose of the rules in this subpart is to implement section 222 of the Communications Act of 1934, as amended, 47 U.S.C. 222."). The FCC also regularly releases CPNI orders that promulgate rules implementing its express statutory obligations. *See* 2007 CPNI Order and 2013 CPNI Order.

includes rules "designed to ensure that telecommunications carriers establish effective safeguards to protect against unauthorized use or disclosure of CPNI."[51] The FCC specifically recognizes that "[a]bsent carriers' adoption of adequate security safeguards, consumers' sensitive information… can be disclosed to third parties without consumers' knowledge or consent."[52] In a 2013 order, the FCC "clarif[ied] existing law so that consumers will know that *their carriers must safeguard these kinds of information so long as the information is collected by or at the direction of the carrier and the carrier or its designee*[53] *has access to or control over the information*."[54]

99. Pursuant to these rules, AT&T must "implement a system by which the status of a customer's CPNI approval can be clearly established *prior to* the use of CPNI."[55] AT&T is also required to "design their customer service records in such a way that the status of a customer's CPNI approval can be clearly established."[56] The FCC's rules also "require carriers to maintain records that track access to customer CPNI records."[57]

100. Upon information and belief, AT&T has failed to implement such a system. The fact that Mr. Shapiro's account was accessed without his authorization on at least four separate occasions demonstrates AT&T's failures in this regard.

101. AT&T's failures are particularly egregious because Mr. Shapiro contacted AT&T following each SIM swap attack and provided specific instructions that employees were not to access his CPNI without his express, prior

[51] 2007 CPNI Order ¶ 9; *see also Id.* at ¶ 35; 47 U.S.C. § 222(c); 47 C.F.R. § 64.2009.
[52] *Id.*
[53] In the ruling, "designee" is defined as "an entity to which the carrier has transmitted, or directed the transmission of, CPNI or is the carrier's agent." *Id.* n. 1.
[54] *Id.* at ¶ 1 (emphasis added).
[55] 2007 CPNI Order ¶¶ 8-9 (emphasis added); *see also* 47 C.F.R. § 64.2009(a).
[56] *Id.* ¶ 9.
[57] *Id.*

approval, as established through the use of passcodes. Mr. Shapiro was told that specific warnings would be placed on his account to this affect. These instructions and warnings were ineffective, as shown by the repeated breaches of Mr. Shapiro's account.

102. AT&T is also required to "train their personnel as to when they are and are not authorized to use CPNI, and carriers must have an express disciplinary process in place."[58]

103. Upon information and belief, AT&T has failed to properly train and supervise their personnel, as reflected by AT&T personnel's involvement in Mr. Shapiro's breaches.

104. Carriers must "maintain a record of all instances where CPNI was disclosed or provided to third parties, or where third parties were allowed access to CPNI."[59]

105. Upon information and belief, AT&T has failed to maintain such a record, as demonstrated by its repeated failure to protect Mr. Shapiro after his CPNI was provided to third-parties.

106. AT&T has also breached its duty to safeguard Mr. Shapiro's CPNI from data breaches, in violation of Section 222(a) and Section 201(b) of the FCA.

107. The FCC has "[made] clear that carriers' existing statutory obligations to protect their customers' CPNI include[s] a requirement that carriers take reasonable steps, which may include encryption, to protect their CPNI databases from hackers and other unauthorized attempts by third parties to access CPNI."[60]

108. AT&T failed to take reasonable steps to protect Mr. Shapiro's CPNI, thereby allowing third-party hackers to access his CPNI on at least four occasions.

[58] 47 C.F.R. § 64.2009(b).
[59] *Id.*; *see also* 47 C.F.R. § 64.2009(c).
[60] 2007 CPNI Order ¶ 36 (citation omitted).

109. The FCC also requires that carriers inform customers – and law enforcement – "whenever a security breach results in that customer's CPNI being disclosed to a third party without that customer's authorization."[61] This requirement extends to any unauthorized disclosure.

110. In adopting this requirement, the FCC rejected the argument that it "need not impose new rules about notice to customers of unauthorized disclosure because competitive market conditions will protect CPNI from unauthorized disclosure."[62]

111. Instead, the FCC found that "[i]f customers and law enforcement agencies are unaware of [unauthorized access], unauthorized releases of CPNI will have little impact on carriers' behavior, and thus provide little incentive for carriers to prevent further unauthorized releases. By mandating the notification process adopted here, we better empower consumers to make informed decisions about service providers and assist law enforcement with its investigations. This notice will also empower carriers and consumers to take whatever 'next steps' are appropriate in light of the customer's particular situation."[63] The FCC specifically recognized that this notice could allow consumers to take precautions or protect themselves "to avoid stalking or domestic violence."[64]

112. AT&T failed in its duty to safeguard Mr. Shapiro's CPNI from breaches and, upon information and belief, has failed to properly inform him of such breaches when they occurred. Mr. Shapiro only received any documentation alerting him that his CPNI had been breached after the *third* hack; he received no such notice following the first two SIM swap attacks. Additionally, he only received documentation for three out of four total attacks.

---

[61] 2007 CPNI Order at ¶ 26; *see also* 47 C.F.R § 64.2011(c).
[62] 2007 CPNI Order ¶ 30.
[63] *Id.*
[64] *Id.* at n. 100.

113. Under the FCA, AT&T is not just liable for its own violations of the Act, but also for violations that it "cause[s] or permit[s]."[65] By failing to secure Mr. Shapiro's account and protect his CPNI, AT&T caused and/or permitted Mr. Shapiro's CPNI to be accessed and used by its own employees and by third-party hackers.

114. AT&T is also responsible for the acts, omissions, and/or failures of officers, agents, employees, or any other person acting for or employed by AT&T, including employees Jack and White.

D. Mr. Shapiro's Harm was Caused by AT&T's Negligence.

115. By failing to secure Mr. Shapiro's account—and protect the confidential and sensitive data contained therein—and to properly hire, train, and supervise their employees, AT&T is responsible for the foreseeable harm Mr. Shapiro suffered as a result of AT&T's negligence.

116. Further, AT&T is responsible for its employees' participation in the conspiracy to rob Mr. Shapiro, as such actions were within the scope of their employment with AT&T. On information and belief, AT&T employees were tasked with and able to change customers' SIM cards.

117. Additionally, AT&T employees' breach of Mr. Shapiro's account and the subsequent SIM swaps were foreseeable. AT&T knew or should have known that Mr. Shapiro's account was at risk, but nonetheless failed to secure his account and failed to properly supervise and train its employees.

118. AT&T has known for more than a decade that third parties frequently attempt to access wireless customers' accounts for fraudulent purposes. In 2007,

[65] *See* 47 U.S.C.A. § 206 (establishing that "[i]n case any common carrier shall do, or cause or permit 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[.]")

the FCC issued an order strengthening its CPNI rules in response to the growing practice of "pretexting."[66] Pretexting is "the practice of pretending to be a particular customer or other authorized person in order to obtain access to that customer's call detail or other private communication records."[67] This 2007 Order put AT&T on notice that its customers' accounts were vulnerable targets of the third-parties seeking unauthorized access.

119. AT&T also knew, or should have known, about the risk SIM swap crimes presented to its customers. SIM swap crimes have been a widespread and growing problem for years. The U.S. Fair Trade Commission ("FTC") reported in 2016 that there were 1,038 reported SIM swap attacks *per month* in January 2013, which increased sharply to 2,658 per month by January 2016—2.5 times as many.[68] The FTC reported that SIM swaps represented 6.3% of all identity thefts reported to the agency in January 2016, and that such thefts "involved all four of the major mobile carriers" – including AT&T.[69]

120. AT&T knew or should have known that it needed to take steps to protect its customers. The FTC's 2017 Report stated that "*mobile carriers are in a better position than their customers to prevent identity theft through mobile account hijacking*[.]"[70] The FTC urged carriers such as AT&T to "adopt a multi-level approach to authenticating both existing and new customers and require their own employees as well as third-party retailers to use it for all transactions."[71] The FTC also specifically warned carriers, including AT&T, of the risk that, due to text

[66] 2007 CPNI Order.
[67] *Id.* at ¶ 1.
[68] Lori Cranor, FTC Chief Technologist, "Your mobile phone account could be hijacked by an identity thief," Federal Trade Commission (June 7, 2016), *available at* https://www.ftc.gov/news-events/blogs/techftc/2016/06/your-mobile-phone-account-could-be-hijacked-identity-thief (hereafter, "2017 FTC Report").
[69] *Id.*
[70] *Id.* (emphasis added).
[71] *Id.*

message password reset requests and two-factor authentication, SIM swapping put subscribers at risk of financial loss and privacy violations:

> Having a mobile phone account hijacked can waste hours of a victim's time and cause them to miss important calls and messages. However, this crime is particularly problematic due to the growing use of text messages to mobile phones as part of authentication schemes for financial services and other accounts. The security of two-factor authentication schemes that use phones as one of the factors relies on the assumption that someone who steals your password has not also stolen your phone number. *Thus, mobile carriers and third-party retailers need to be vigilant in their authentication practices to avoid putting their customers at risk of major financial loss and having email, social network, and other accounts compromised.*[72]

121. AT&T admitted it was aware of SIM swap crimes and the effect they could have on its customers in September 2017 when AT&T's Vice President of Security Platforms published an article on AT&T's "Cyber Aware" blog about SIM swaps.[73] In the article, AT&T acknowledged that subscribers with "valuable accounts that are accessible online" are likely targets of SIM swaps. AT&T recommended that its customers set up passcodes that would provide "extra security." These passcodes repeatedly failed to protect Mr. Shapiro.

122. AT&T therefore knew that its customers' accounts were at risk *at least* 8 months before *any* breaches of Mr. Shapiro's account. At the time of his first attack in May 2016, Mr. Shapiro informed AT&T—both on the phone and in person—that he had valuable online accounts, thereby making him the type of individual that AT&T recognized was specifically vulnerable to SIM swap attacks. Nonetheless, AT&T failed to take reasonable steps to protect his account.

---

[72] *Id.* (emphasis added).

[73] Brian Rexroad, "Secure Your Number to Reduce SIM Swap Scams," AT&T's Cyber Aware (Sep. 2017), *available at* https://about.att.com/pages/cyberaware/ni/blog/sim_swap.

123. AT&T's inadequate security procedures are particularly egregious in light of AT&T's repeated public statements about the importance of cyber security and its public representations about its expertise in this area. AT&T has an entire series on its public YouTube channel ("AT&T ThreatTraq") dedicated to discussing and analyzing emerging cybersecurity threats.[74] In its videos, AT&T describes itself as a "network that senses and mitigates cyber threats."[75]

124. AT&T recognizes the risks that arise when a cell phone is compromised, stating, "Our phones are mini-computers, and with so much personal data on our phones today, it's also important to secure our mobile devices."[76] AT&T's advertisements also stress how central a role cell phones play in its customer's lives, stating: "My phone is my life" and "My phone is everything." The same ad stresses how the inability to use a cell phone makes people feel "completely untethered, flailing around."[77]

125. AT&T markets its ability to identify to and neutralize emerging cyber threats for its customers. In one video, AT&T employees discuss "threat hunting" which they describe as "an active threat analysis where you're actually thinking about your adversary."[78] They claim that it's "important" and "something [AT&T has] been doing for a long time."[79] They advise that companies should think about "what would a hacker want to do, where would a hacker go to get my data, what are some of the points on my network that are most vulnerable, or where is the data

[74] "AT&T Tech Channel," YouTube, *available at* https://www.youtube.com/user/ATTTechChannel.
[75] "AT&T – Protect Your Network with the Power of &," VIMEO, *available at* https://vimeo.com/172399153.
[76] AT&T, "Mobile Security," YOUTUBE (Feb. 12, 2019), *available* at https://www.youtube.com/watch?v=KSPHS89VnX0.
[77] "AT&T Mobile Movement Campaign – Ads," VIMEO, *available at* https://vimeo.com/224936108.
[78] AT&T Tech Channel, "The Huntin' and Phishin' Episode," YOUTUBE (Apr. 21, 2017), *available at* https://www.youtube.com/watch?v=3g9cPCiFosk.
[79] *Id.*

flow that is potentially going to be a leakage" and state that "having threat hunting as part of a proactive continuous program, integrating with existing security measures, will help [you] stay ahead of the threats."[80]

126. Not only did AT&T advise staying ahead of and addressing cyber threats, it also stressed that these practices could even help identify "insider threats"—*employees within the company.*

127. In an additional video focused on insider threats, AT&T employees go on at length about the threat of company insiders selling corporate information *and access*, citing a survey showing that "30% [of respondents] had purposefully sent data outside of their organization at some point in time" and "14% of the people that were interviewed said they would actually sell their corporate log-ins to folks on the outside *or sell that data for less than about $250 US.*"[81] They cited as a "significant concern" the "individuals that have privileged access, that have broad access inside an organization."[82] AT&T therefore knew or should have known that there was a significant risk that its own employees would sell AT&T data—including customer account data—and that the risk was heightened when employees had too broad of an access to corporate systems, yet AT&T failed to put sufficient systems and resources in place to mitigate that risk, despite its own advice to the contrary.

128. AT&T has also recognized the danger presented to its customers when their email addresses are hacked, as Mr. Shapiro's was on multiple occasions as a result of AT&T's failures. As one AT&T employee puts it: "I think most people do have something valuable [in their email accounts], which is access to all their other

[80] *Id.*
[81] AT&T ThreatTraq, "The Real Threat of Insider Threats," YouTube (May 5, 2017), *available at* https://www.youtube.com/watch?v=ZM5tuNiVsjs (emphasis added).
[82] *Id.*

accounts, which you can get with a password reset."[83] They call this "something worth keeping safe."[84] They advised that a "strong, obviously, security awareness program within a company… is extremely important."[85]

129. In this video series, AT&T makes specific mentions of SIM swapping activity. In one video, AT&T's Vice President of Security Platforms (Brian

Rexroad) and Principal of Technology Security (Matt Keyser) discuss the hack of a forum called OGusers. [86] In the segment, they discuss the hacking of social media users' account names and point to a news story that highlights—in distinct orange type—that OGusers is a forum popular among people "conducting SIM swapping attacks to seize control over victims' phone numbers."[87]

Figure 2

[83] *Id.*
[84] *Id.*
[85] *Id.*
[86] AT&T ThreatTraq, "5/31/19 Account-hacking Forum OGusers Hacked," YOUTUBE (May 31 2019), *available at* https://www.youtube.com/watch?time_continue=234&v=cS4xV3cej3A.
[87] *Id.*; *see also* Freeman Indictment at ¶ 2 (Describing how "discussions—such as discussing the manner and means to [SIM swap] attacks generally, and networking among [SIM swap hackers]—typically took place on forums such as "OGusers.").

130. AT&T was therefore well aware of the significant risk that AT&T employees and SIM swapping presented to its customers, and the need to mitigate such risks, but nonetheless failed to take adequate steps to protect Mr. Shapiro. Instead, it continued to make public statements giving rise to a reasonable expectation that AT&T could—and would—protect its customers.

131. Additionally, Mr. Shapiro's hack was foreseeable because at least two of the AT&T employees involved—Jack and White—were involved in a suspiciously high number of unauthorized SIM swaps the very same month of Mr. Shapiro's first and second hacks. White conducted 29 *unauthorized SIM swaps* in May 2018, while Jack conducted *12 unauthorized swaps* that same month. This suspicious activity should have raised alarms at AT&T, but the company nonetheless failed to protect Mr. Shapiro from these employees.

132. The risk to Mr. Shapiro's account, specifically, was particularly foreseeable after the very first breach on May 16, 2018. Despite confirming that a breach had occurred, AT&T employees refused to help Mr. Shapiro when his account was again breached and his SIM card swapped just a few minutes after he restored control over his account on May 16. Instead, AT&T did nothing while its employees aided hackers in their more than $1.8 million theft from Mr. Shapiro.

133. Even after *two* documented account breaches and unauthorized SIM swaps in May, AT&T failed to protect Mr. Shapiro's account on *two* additional occasions in November 2018 and May 2019.

134. That Mr. Shapiro was at risk of account breaches at the hands of AT&T employees is particularly foreseeable—and AT&T's failures are particularly stark—in light of AT&T's history of unauthorized employee access to customer accounts.

135. In 2015, AT&T faced an FCC enforcement action, and paid a $25 million civil penalty, for nearly identical failures to protect its customers' sensitive

account data.[88] In that case, as AT&T admitted, employees at an AT&T call center breached 280,000 customers' accounts.[89] Specifically, AT&T employees had improperly used login credentials to access customer accounts and access customer information that could be used to unlock the customers' devices.[90] The employees then sold the information they obtained from the breaches to a third party.[91]

136. The FCC concluded that AT&T's "failure to reasonably secure customers' proprietary information violates a carrier's statutory duty under the Communications Act to protect that information, and also constitutes an unjust and unreasonable practice in violation of the Act."[92]

137. The FCC stressed that the FCA is intended to "ensure that consumers can trust that carriers have taken appropriate steps to ensure that unauthorized persons are not accessing, viewing or misusing their personal information."[93] It stressed its expectation that "telecommunications carriers such as AT&T… take 'every reasonable precaution' to protect their customers' data[.]"[94]

138. As part of its penalty, AT&T entered into a stipulated Consent Decree with the FCC, in which AT&T agreed to develop and implement a compliance plan to ensure appropriate safeguards to protect consumers against similar breaches by improving its privacy and data security practices.[95]

139. This FCC enforcement action underscores AT&T's knowledge of the risk its employees presented to customers, the prevalence of employee breaches to customer data, the sensitive nature of customer CPNI, and its duties to protect and safeguard that data.

---

[88] *In the Matter of AT&T Servs., Inc.*, 30 F.C.C. Rcd. 2808 (2015).
[89] *Id.* at ¶ 1.
[90] *Id.* at ¶¶ 7, 11.
[91] *Id.* at ¶ 1.
[92] *Id.* at ¶ 2.
[93] *Id.*
[94] *Id.*
[95] *Id.* at ¶¶ 2, 17-18, 21.

140. Nonetheless, more than 3 years after stipulating to the Consent Decree, AT&T still failed to protect its customer from employee breaches of customer CPNI and other account data, virtually identical to the breaches at issue here, heightening the degree of its negligence.

141. Mr. Shapiro, unlike AT&T, was not in a position to adequately protect himself from the harms arising from the SIM swap attacks. AT&T, Mr. Shapiro's wireless provider, was responsible for safeguarding his account and its involvement was required for any change in SIM to be effective. Because SIM change requests were all routed through AT&T, and not through Mr. Shapiro directly, AT&T alone was positioned to prevent unauthorized SIM changes. It is unreasonable to expect Mr. Shapiro to be able to fully protect his account when AT&T, the responsible entity, failed to do so.

142. Additionally, Mr. Shapiro took all of the steps that AT&T advised he take in order to protect his account—including changing his account passcode—and was repeatedly told by AT&T that such steps would protect his account from further breaches and SIM swaps. Mr. Shapiro reasonably relied on these representations.

i. **AT&T is Liable for the Acts of its Employees.**

143. AT&T is liable for the acts of its employees, including Jack and White, who facilitated the unauthorized access to, and resulting theft from, Mr. Shapiro.

144. AT&T failed to put in place adequate systems and procedures to prevent the unauthorized employee access to and sale of Mr. Shapiro's account and related data. AT&T failed to properly hire and supervise its employees, allowing them to access Mr. Shapiro's sensitive and confidential account data, and sell access to his account and that data to third parties.

145. In the context of AT&T's enterprise as a telecommunications carrier, an employee accessing a customer's account information and effectuating a SIM swap—even without authorization—is not so unusual or startling that it would not be unfair to include the loss resulting from such unauthorized access among other costs of AT&T's business – particularly in light of AT&T's awareness of the risk of SIM swaps to its customers.

146. Further, imposing liability on AT&T may prevent recurrence of SIM swap behavior because it creates a strong incentive for vigilance and proper safeguarding of customers' data by AT&T—which is the sole party in the position to guard substantially against this activity, as it is the custodian and guardian of this data.

147. As a customer of AT&T, Mr. Shapiro is entitled to rely upon the presumption that AT&T and the agents entrusted with the performance of AT&T's business have faithfully and honestly discharged the duty owed to him by AT&T, and that they would not knowingly gain unauthorized access to his account in order to aid in perpetuating a theft from him.

148. The reasonableness of Mr. Shapiro's expectations that AT&T would safeguard his data is confirmed by the fact that the federal agency responsible for overseeing AT&T's duties to its customers, the FCC, has stated that it "fully expect[s] carriers to take every reasonable precaution to protect the confidentiality of proprietary or personal customer information."[96]

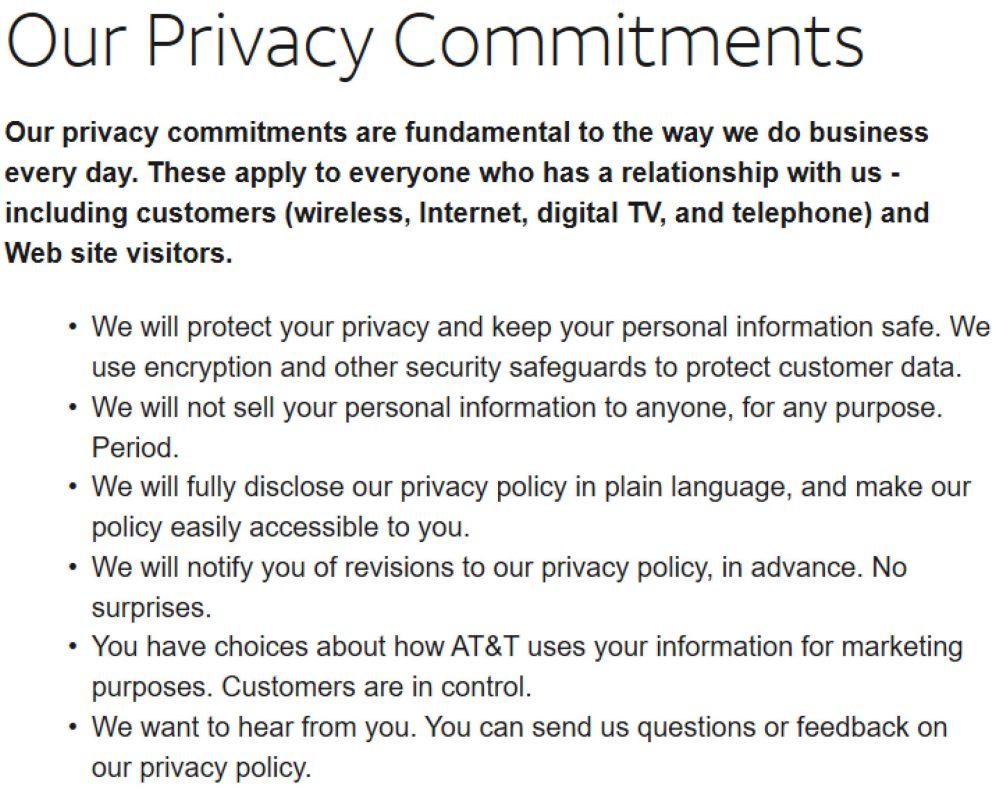
C. AT&T's Misrepresentations and Omissions.

149. AT&T's Privacy Policy, and the "Privacy Commitments" included therein, falsely represents and fails to disclose material information about its data security practices.

[96] 2007 CPNI Order ¶ 64.

150. In its Privacy Policy, AT&T promised to protect Mr. Shapiro's privacy and personal information, including by using "security safeguards." AT&T further pledges that it will not sell customer data.

151. These representations created an expectation that Mr. Shapiro's AT&T account and associated data would be safe and secure, that employees would not access his account without authorization or sell access to his account, that his data would be protected from unauthorized disclosure, and that he could control how and when his data was accessed. Figure 3, immediately below, is an excerpt from AT&T's Privacy Policy.



Our Privacy Commitments

Our privacy commitments are fundamental to the way we do business every day. These apply to everyone who has a relationship with us - including customers (wireless, Internet, digital TV, and telephone) and Web site visitors.

- We will protect your privacy and keep your personal information safe. We use encryption and other security safeguards to protect customer data.
- We will not sell your personal information to anyone, for any purpose. Period.
- We will fully disclose our privacy policy in plain language, and make our policy easily accessible to you.
- We will notify you of revisions to our privacy policy, in advance. No surprises.
- You have choices about how AT&T uses your information for marketing purposes. Customers are in control.
- We want to hear from you. You can send us questions or feedback on our privacy policy.

Figure 3[97]

152. AT&T's representation that it "uses encryption and other security safeguards to protect customer data" is false and misleading.

153. As alleged fully above, AT&T allowed its employees to access Mr. Shapiro's account, and the CPNI and other sensitive data contained therein,

[97] "Privacy Policy," AT&T, attached hereto as Exhibit G.

without his authorization. AT&T's statement that it would use encryption and other security safeguards to protect customers' data is therefore a material misrepresentation.

154. Upon information and belief, AT&T's security safeguards were inadequate, including its system which—upon information and belief—allowed an individual employee to conduct SIM swaps without adequate oversight, even when that employee conducted a large number of unauthorized SIM swaps in a short period of time (as demonstrated in the cases of White and Jack).

155. "Having one employee who can conduct these SIM swaps without any kind of oversight seems to be the real problem," says Lieutenant John Rose, a member of the California-based Regional Enforcement Allied Computer Team ("REACT"), a multi-jurisdictional law enforcement partnership specializing in cybercrime.[98] "And it seems like [the carriers] could really put a stop to it if there were more checks and balances to prevent that. It's still very, very easy to SIM swap, and something has to be done because it's just too simple. Someone needs to light a fire under some folks to get these protections put in place."[99]

156. AT&T failed to put in place adequate systems and procedures to prevent the unauthorized employee access to and sale of Mr. Shapiro's account and related data. In connection with subsequent criminal investigations into Mr. Shapiro's SIM swaps, AT&T informed law enforcement that it had the capacity to see how many different SIM cards had been associated with the same single cell phone's IMEI. In other words, AT&T could see when one cell phone had multiple SIM cards associated with it in a short amount of time.[100]

---

[98] "Busting SIM Swappers and SIM Swap Myths," KREBSONSECURITY (Nov. 18, 2018), *available at* https://krebsonsecurity.com/2018/11/busting-sim-swappers-and-sim-swap-myths.

[99] A REACT investigative report, (attached hereto as Exhibit I), describes how certain SIM swap attacks occurred, and includes statements from victims, including Mr. Shapiro, at p. 11-12.

[100] *See* Probation Report, *California v. Joel Ortiz*, No. C-189481 (CA Sup. Ct. March 14, 2019) at p. 7 (attached hereto as Exhibit H.)

157. AT&T also informed law enforcement that the hacker involved in Mr. Shapiro's SIM swap had requested that *40 different AT&T wireless accounts* be moved onto his phone (identified by its IMEI number) in the months leading up to Mr. Shapiro's swap.[101] AT&T therefore had the technology to track how many different accounts were being much on to the same telephone, as demonstrated by its ability to pull this information for law enforcement. Despite its ability to track this highly suspicious behavior, AT&T failed to use this technology to protect Mr. Shapiro's account. If AT&T had proper security safeguards in place, it would have recognized this behavior, flagged it as suspicious, and prevented any further SIM swaps onto that phone – thereby protecting Mr. Shapiro.

158. AT&T provided information to law enforcement about how AT&T SIM swap victims' AT&T accounts were used while under the control of hackers. This information clearly showed that hackers were using the AT&T wireless accounts to attempt to access other personal accounts. AT&T informed law enforcement that, "During the time the [hacker] controlled several of the [SIM swap] victims' cell telephones, all telephones received multiple text messages while no text messages were sent."[102] This was suspicious because it indicated that hackers were receiving password-reset or two-factor authentication text messages in an attempt to access victims' other online accounts, rather than using the AT&T accounts for normal, legitimate purposes. As described by law enforcement:

> Based on the volume of text messages the [hacker] received, the short time he controlled the [AT&T user] victims' accounts, as well as the majority of text messages originating from short code numbers,[103] [law enforcement] officers deduced [that] once [the hacker' gained control of a victim's cell phone account, the

[101] *Id.* at 7.
[102] *Id.*
[103] As described by law enforcement, a "short code number" is "a phone number used strictly to send text message and cannot receive voice calls." Short code numbers are used by businesses to send users password-reset links or passcodes.

> [hacker] attempted to log into their other accounts. Police believed the defendant was able to do this either by receiving a 2FA [two-factor authentication] text message from individual websites sent via text message to the AT&T account controlled by the [hacker], or the specific website text a code allowing the [hacker] to reset the passwords on-line.[104]

159. Therefore, AT&T had the capability to see this behavior, and should have flagged it as suspicious. If AT&T had proper security safeguards in place, it would have recognized this behavior, flagged it as suspicious, and prevented any further SIM swaps onto that phone – thereby protecting Mr. Shapiro.

160. Additionally, as alleged fully above, AT&T failed to establish a consent mechanism that verified proper authorization before Mr. Shapiro's data was accessed and provided to third parties. AT&T's statement that it would use encryption and other security safeguards to protect customers' data is therefore a material misrepresentation.

161. AT&T's representation that it "will protect [customers'] privacy and keep [their] personal information safe" is false and misleading.

162. As alleged fully above, AT&T failed to establish a consent mechanism that verified proper authorization before Mr. Shapiro's account and the data therein was used without his authorization or consent, and disclosed to third parties. Mr. Shapiro's privacy and personal information was not safe, as demonstrated by the repeated breaches of his AT&T account. AT&T's statement that it would protect customers' privacy and keep their personal information safe is therefore a material misrepresentation.

163. AT&T's representation that it "will not sell [customers'] personal information to anyone, for any purpose. Period" is false and misleading.

[104] Ex. H at 9.

164. As alleged fully above, AT&T employees sold access to Mr. Shapiro's AT&T account to third parties. AT&T's statement that it would not sell customers' personal information is therefore a material misrepresentation.

165. AT&T also makes numerous false or misleading representations concerning its treatment of customers' data that qualifies as CPNI under the FCA.

166. AT&T explicitly and falsely represents in its Privacy Policy that it does not "sell, trade or share" their CPNI:

> We do not sell, trade or share your CPNI with anyone outside of the AT&T family of companies* or our authorized agents, unless required by law (example: a court order).[105]

167. As alleged fully above, AT&T provided access to Mr. Shapiro's CPNI to third-party hackers. This use was not required by law and was instead *prohibited* by law.

168. AT&T also states that it only uses CPNI "internally" and its *only* disclosed use of CPNI is "among the AT&T companies and our agents in order to offer you new or enhanced services."[106]

169. AT&T employees' sale of access to Mr. Shapiro's account and related data as described herein was not for "internal" AT&T purposes, nor was it used to market AT&T services. AT&T's statements regarding the sale and/or use of customer CPNI are therefore material misrepresentations. Its failure to disclose this sale of access to CPNI is a material omission.

[105] "Customer Proprietary Network Information (CPNI)," Ex. G at p. 31-32. The "AT&T family of companies" is defined "those companies that provide voice, video and broadband-related products and/or services domestically and internationally, including the AT&T local and long distance companies, AT&T Corp., AT&T Mobility, DIRECTV, and other subsidiaries or affiliates of AT&T Inc. that provide, design, market, or sell these products and/or services." *Id.*
[106] *Id.*

170. AT&T also falsely represents that it "uses technology and security features, and strict policy guidelines with ourselves and our agents, to safeguard the privacy of CPNI."

171. As alleged fully above, AT&T and its agents failed to safeguard Mr. Shapiro's CPNI. Instead, it stored customer CPNI in such a way that unauthorized access was easily obtained by employees and third parties. AT&T's statements regarding the technology and security features it uses to safeguard customer CPNI are therefore material misrepresentations.

172. After each breach of his account and unauthorized SIM swap, AT&T repeatedly, and falsely, represented to Mr. Shapiro that his account was safe from future breaches. In reliance upon these statements, Mr. Shapiro maintained his AT&T account. AT&T also repeatedly told Mr. Shapiro that the notations made on his account and the passcode needed to change his SIM card would protect him from future breaches and SIM swaps. These misrepresentations were false and materially misleading, as demonstrated by the ongoing breaches to Mr. Shapiro's account.

173. AT&T was obligated to disclose the weaknesses and failures of its account and data security practices, as AT&T had exclusive knowledge of material facts not known or knowable to its customers, AT&T actively concealed these material facts from Mr. Shapiro, and such disclosures were necessary to materially qualify its representations that it did not sell and took measures to protect consumer data and to materially qualify its partial disclosures concerning its use of customers' CPNI. Further, AT&T was obligated to disclose its practices under the FCA.

174. A reasonable person would be deceived and misled by AT&T's misrepresentations, which clearly indicated that AT&T would not sell, and would in fact safeguard, its customers' personal information and CPNI.

175. AT&T intentionally misled Mr. Shapiro regarding its data security practices in order to maintain his business and evade prosecution for its unlawful acts.

176. AT&T's representations that it protected customers' personal information, when in fact it did not, were false, deceptive, and misleading and therefore a violation of the FCA.

VI. CLAIMS FOR RELIEF

COUNT I
Violations of The Federal Communications Act, 47 U.S.C. § 201 *et seq.*

177. Plaintiff Mr. Shapiro realleges and incorporates all of the preceding paragraphs as though fully set forth in this cause of action.

178. AT&T has violated 47 U.S.C. § 222(a) by failing to protect the confidentiality of Mr. Shapiro's CPNI, as detailed herein.

179. AT&T has violated 47 U.S.C. § 222(c) by using, disclosing, and/or permitting access to Mr. Shapiro's CPNI without the notice, consent, and/or legal authorization required under the FCA, as detailed herein. AT&T also caused and/or permitted third parties to use, disclose, and/or permit access to Mr. Shapiro's CPNI without the notice, consent, and/or legal authorization required under the FCA, as detailed herein.

180. As fully alleged above, Mr. Shapiro has suffered injury to his person, property, health, and reputation as a consequence of AT&T's violations of the FCA. Additionally, Mr. Shapiro has suffered emotional damages, including severe anxiety and depression, mental anguish, and suffering as a result of AT&T's acts and practices.

181. Mr. Shapiro seeks the full amount of damages sustained as a consequence of AT&T's violations of the FCA, together with reasonable attorneys' fees, to be fixed by the Court and taxed and collected as part of the costs of the case. Mr. Shapiro also moves for a writ of injunction or other proper process,

mandatory or otherwise, to restrain Defendant AT&T and its officers, agents, or representatives from further disobedience of the 2007 and 2013 CPNI Orders, or to compel their obedience to the same.

COUNT II
Violations of The California Unfair Competition Law ("UCL") under the Unlawful, Unfair and Fraudulent Prongs,
California Business & Professional Code § 17200 *et seq*.

182. Plaintiff Mr. Shapiro realleges and incorporates all of the preceding paragraphs as though fully set forth in this cause of action.

183. California's Unfair Competition Law (UCL) prohibits any "unlawful, unfair or fraudulent business act or practice." AT&T's business acts and practices complained of herein were unlawful, unfair, and fraudulent.

184. AT&T made material misrepresentations and omissions concerning its sale of access to and safeguarding of Mr. Shapiro's CPNI. As alleged fully above, a reasonable person would attach importance to the privacy of his sensitive account data in determining whether to contract with a wireless cell phone provider.

185. AT&T had a duty to disclose the nature of its inadequate security practices and failures in hiring, training, and supervising staff. AT&T had exclusive knowledge of material facts not known or knowable to its customers and AT&T actively concealed these material facts from its customers.

186. Further, additional disclosures were necessary to materially qualify AT&T's representations that it did not sell consumer data and took measures to protect that data, and its partial disclosures concerning its use of customers' CPNI. AT&T was obligated to disclose its practices, as required by the FCA. The

magnitude of the harm suffered by Mr. Shapiro underscores the materiality of AT&T's omissions.

187. A reasonable person, such as Mr. Shapiro, would be deceived and misled by AT&T's misrepresentations, which indicated that AT&T would not sell, and would in fact safeguard, its customers' personal and proprietary information.

188. AT&T intentionally misled its customers regarding its data protection practices in order to attract customers and evade prosecution for its unlawful acts. Indeed, AT&T told Mr. Shapiro after each SIM swap attack that his account would be safe from future breaches, and in reliance on those assurances, Mr. Shapiro did not close his AT&T wireless account.

189. AT&T's actions detailed herein constitute an unlawful business act or practice. As alleged herein, AT&T's conduct is a violation of the California constitutional right to privacy, the FCA, and the CLRA.

190. AT&T's actions detailed herein constitute an unfair business act or practice.

191. AT&T's conduct lacks reasonable and legitimate justification in that Mr. Shapiro has been misled as to the nature and integrity of AT&T's goods and services and has suffered injury as a result.

192. The gravity of the harm caused by AT&T's practices far outweigh the utility of AT&T's conduct. AT&T's practices were contrary to the letter and spirit of the FCA and its corresponding regulations, which require cell carriers to disclose customers' CPNI only upon proper notice, consent, and authorization, and aims to vest carrier customers with control over their data. Due to the surreptitious nature of AT&T's actions, Mr. Shapiro could not have reasonably avoided the harms incurred as a result.

193. As the FCA establishes, it is against public policy to allow carrier employees or other third parties to access, use, or disclose telecommunications

customers' sensitive account information. The effects of AT&T's conduct are comparable to or the same as a violation of the FCA.

194. AT&T's actions detailed herein constitute a fraudulent business act or practice.

195. As established herein, Mr. Shapiro has suffered economic harm as a result of AT&T's unfair competition. Additionally, had AT&T disclosed the true nature and extent of its data security and protection practices—and the flaws inherent in its systems—and its unwillingness to properly protect its customers, Mr. Shapiro would not have subscribed to or paid as much money for AT&T's wireless services.

196. Mr. Shapiro seeks injunctive and declaratory relief for AT&T's violations of the UCL. Mr. Shapiro seeks public injunctive relief against AT&T's unfair and unlawful practices in order to protect the public and restore to the parties in interest money or property taken as a result of AT&T's unfair competition. Mr. Shapiro seeks a mandatory cessation of AT&T's practices.

COUNT III
Violations of the California Constitutional Right to Privacy

197. Mr. Shapiro realleges and incorporates all of the preceding paragraphs as though fully set forth in this cause of action.

198. The California Constitution declares that, "All people are by nature free and independent and have inalienable rights. Among these are enjoying and defending life and liberty, acquiring, possessing, and protecting property, and pursuing and obtaining safety, happiness, and privacy." Cal. Const. Art. I, § 1.

199. Mr. Shapiro has a reasonable expectation of privacy in his mobile device and his AT&T account information.

200. AT&T intentionally intruded on and into Mr. Shapiro's solitude, seclusion, or private affairs by allowing its employees and third parties to

improperly access Mr. Shapiro's confidential AT&T account information without proper consent or authority.

201. The reasonableness of Mr. Shapiro's expectations of privacy is supported by AT&T and its agents' unique position to safeguard his account data, including the sensitive and confidential information contained therein, and protect Mr. Shapiro from SIM swap attacks.

202. AT&T and its agents' intrusions into Mr. Shapiro's privacy are highly offensive to a reasonable person. This is evidenced by federal legislation enacted by Congress and rules promulgated and enforcement actions undertaken by the FCC aimed at protecting AT&T customers' sensitive account data from unauthorized use or access.

203. The offensiveness of AT&T's conduct is heightened by its material misrepresentations to Mr. Shapiro concerning the safety and security of his account.

204. Mr. Shapiro suffered great personal and financial harm by the intrusion into his private affairs, as detailed throughout this Complaint.

205. AT&T's actions and conduct complained of herein were a substantial factor in causing the harm suffered by Mr. Shapiro. But for AT&T employees' involvement in a conspiracy to rob Mr. Shapiro, and AT&T's failure to protect Mr. Shapiro from such harm through adequate security and oversight systems and procedures, Mr. Shapiro would not have had his personal privacy repeatedly violated and would not have been a victim of SIM swap theft.

206. As a result of AT&T's actions, Mr. Shapiro seeks nominal and punitive damages in an amount to be determined at trial. Mr. Shapiro seeks punitive damages because AT&T's actions were malicious, oppressive, willful. AT&T knew or should have known about the risks faced by Mr. Shapiro, and the grave consequences of such risks. Nonetheless, AT&T utterly failed to protect Mr.

Shapiro – instead allowing its employees to profit to his detriment. Punitive damages are warranted to deter AT&T from engaging in future misconduct.

COUNT IV
Negligence

207. Mr. Shapiro realleges and incorporates all of the preceding paragraphs as though fully set forth in this cause of action.

208. AT&T owed a duty to Mr. Shapiro—arising from the sensitivity of his AT&T account information and the foreseeability of harm to Mr. Shapiro should AT&T fail to safeguard and protect such data—to exercise reasonable care in safeguarding his sensitive personal information. This duty included, among other things, designing, maintaining, monitoring, and testing AT&T's and its agents', partners', and independent contractors' systems, protocols, and practices to ensure that Mr. Shapiro's information was adequately secured from unauthorized access.

209. Federal law and regulations, as well as AT&T's privacy policy, acknowledge AT&T's duty to adequately protect Mr. Shapiro's confidential account information.

210. AT&T owed a duty to Mr. Shapiro to protect his sensitive account data from unauthorized use, access, or disclosure. This included a duty to ensure that his CPNI was only used, accessed, or disclosed with proper consent.

211. AT&T owed a duty to Mr. Shapiro to implement a system to safeguard against and detect unauthorized access to Mr. Shapiro's AT&T data in a timely manner.

212. AT&T owed a duty to Mr. Shapiro to disclose the material fact that its data security practices were inadequate to safeguard Mr. Shapiro's AT&T account data from unauthorized access by its own employees and others.

213. AT&T had a special relationship with Mr. Shapiro due to its status as his telecommunications carrier, which provided an independent duty of care.

AT&T had the unique ability to protect its systems and the data it stored thereon from unauthorized access.

214. Mr. Shapiro's willingness to contract with AT&T, and thereby entrust AT&T with his confidential and sensitive account data, was predicated on the understanding that AT&T would undertake adequate security and consent precautions.

215. AT&T breached its duties by, *inter alia*: (a) failing to implement and maintain adequate security practices to safeguard Mr. Shapiro's AT&T account and data—including his CPNI—from unauthorized access, as detailed herein; (b) failing to detect unauthorized access in a timely manner; (c) failing to disclose that AT&T's data security practices were inadequate to safeguard Mr. Shapiro's data; (d) failing to supervise its employees and prevent employees from accessing and utilizing Mr. Shapiro's AT&T account and data without authorization; and (e) failing to provide adequate and timely notice of unauthorized access.

216. AT&T was also negligent in its authorization of Mr. Shapiro's SIM card swap. AT&T knew or should have known that at least *forty* different AT&T numbers had been moved to the same cell phone (identified by its IMEI) in the months leading up to Mr. Shapiro's first SIM swap. AT&T knew or should have known that this was highly suspicious. Nevertheless, AT&T effectuated the transfer of Mr. Shapiro's AT&T account to this same cell phone. AT&T had the technical capacity to track this behavior—as reflected in its willingness to do so for law enforcement—but nonetheless failed to utilize it for the benefit and protection of Mr. Shapiro.

217. But for AT&T's breaches of its duties, Mr. Shapiro's data would not have been accessed by unauthorized individuals.

218. Mr. Shapiro was a foreseeable victim of AT&T's inadequate data security practices and consent mechanisms. As alleged fully above, AT&T knew or

should have known that SIM swaps presented a serious threat to its customers, including Mr. Shapiro, before Mr. Shapiro's account was breached for the first time. AT&T also knew or should have known that Mr. Shapiro was at a heightened risk after (1) he informed AT&T employees that he had digital currency accounts, a risk factor AT&T has acknowledged, and (2) he had previously been the target of SIM swap attacks. AT&T also knew that improper procedures and systems to safeguard customer data could allow its employees to authorize customers' accounts and data and sell that to third parties, as occurred in the 2015 FCC enforcement action.

219. AT&T knew or should have known that unauthorized accesses would cause damage to Mr. Shapiro. AT&T admitted that unauthorized account access presents a significant threat to its customers, and became aware during its 2015 FCC enforcement action of the harms caused by unauthorized account access.

220. AT&T's negligent conduct provided a means for unauthorized individuals to access Mr. Shapiro's AT&T account data, take over control of his wireless phone, and use such access to hack into numerous online accounts in order to rob Mr. Shapiro and steal his personal information.

221. As a result of AT&T's failure to prevent unauthorized accesses, Mr. Shapiro suffered grave injury, as detailed herein, including severe emotional distress. This emotional distress arose out of AT&T's breach of its legal duties. The damages Mr. Shapiro suffered were a proximate, reasonably foreseeable result of AT&T's breaches of its duties.

222. Therefore, Mr. Shapiro is entitled to damages in an amount to be proven at trial.

COUNT V
Negligent Supervision and Entrustment

223. Mr. Shapiro realleges and incorporates all of the preceding paragraphs as though fully set forth in this cause of action.

224. AT&T conducts its business activities through employees or other agents, including AT&T contract attorneys.

225. AT&T is liable for harm resulting from its agents' and employees' conduct because AT&T was reckless or negligent in employing and/or entrusting employees—including, but not limited to, White and Jack—in work involving the risk of harm to others, including Mr. Shapiro.

226. As alleged herein, AT&T knew or had reason to believe that its employees—including Jack and/or White—were unfit and nonetheless failed to exercise reasonable care in properly investigating Jack and/or White. AT&T was negligent in supervising these employees and in entrusting them with what it knew to be highly sensitive confidential information. AT&T knew or had reason to know that its employees—including, but not limited to, White and Jack—were likely to harm others in view of the work AT&T entrusted to them.

227. As alleged by law enforcement, White conducted 29 unauthorized SIM swaps and Jack conducted 12 swaps in the same month of Mr. Shapiro's first two SIM swaps. Nonetheless, on information and belief, AT&T failed to take appropriate action to prevent additional harm to its customers, including Mr. Shapiro. Additionally, AT&T was aware that Jack and White had the ability to access its customers' accounts, including Mr. Shapiro's account, and conduct SIM swaps, even without proper customer authorization. Nonetheless, AT&T failed to put any additional protections on customer accounts to prevent such swaps.

228. Upon information and belief, AT&T failed to exercise due care in selecting its employees, and thereby negligently or reckless employed Jack and White to do acts—including accessing customer accounts and effectuating SIM swaps—which necessarily brought them in contact with others, including Mr. Shapiro, while in the performance of those duties.

229. AT&T's acts, as alleged herein, were negligent in that they created the risk of White's and Jack's criminal acts.

230. Unauthorized account access and SIM swapping, the particular risks and hazards that Mr. Shapiro was exposed to, are tied to AT&T's negligence and recklessness in employing, and continuing to employee through the time of Mr. Shapiro's injury, Jack and White.

231. AT&T also failed to properly supervise its employees, and instead continued to negligently entrust them with sensitive customer data. Had AT&T fired Jack and White when they first began to exhibit suspicious SIM swap activity—including but not limited to an irregularly high number of SIM swaps in a short period of time—Mr. Shapiro would not have been injured.

232. Had AT&T built a system to effectively authenticate and verify consumer consent before allowing employees to access their CPNI—as required by the FCA—Mr. Shapiro would not have been injured.

233. Had AT&T prevent individual employees from unilaterally changing customer's SIM swaps without proper oversight, Mr. Shapiro would not have been injured.

234. In sum, AT&T gave its employees the tools and opportunities they needed to gain unauthorized access to Mr. Shapiro's account and failed to prevent them from doing so, thereby allowing them to use AT&T's systems to perpetuate privacy breaches and thefts against Mr. Shapiro.

235. Jack's and/or White's actions have a causal nexus to their employment. Mr. Shapiro's injuries arose out of his contract with AT&T as his carrier, and AT&T's resulting access to his CPNI and account data. The risk of injury to Mr. Shapiro was inherent in the AT&T working environment.

236. Mr. Shapiro's injury was also foreseeable. As alleged fully above, AT&T was aware of the risks that SIM swaps presented to their customers. AT&T

was also aware that its customers' accounts were vulnerable to unauthorized access to and sale by its own employees, as demonstrated in the 2015 FCC enforcement action. AT&T was aware that Mr. Shapiro was at a heightened risk due to his possession of cryptocurrency and the previous unauthorized SIM swaps conducted in his AT&T account. Nonetheless, AT&T failed to take appropriate steps to protect Mr. Shapiro, in violation of its duty.

COUNT VI
Violations of California's Consumers Legal Remedies Act ("CLRA"), California Civil Code § 1750 *et seq.*

237. Mr. Shapiro realleges and incorporates all of the preceding paragraphs as though fully set forth in this cause of action.

238. As an AT&T customer, Mr. Shapiro engaged in transactions with AT&T concerning his wireless service. Mr. Shapiro sought and acquired services from AT&T for his personal, family and household purposes.

239. AT&T has engaged in unfair methods of competition and unfair or deceptive acts or practices intended to result and which did result in the sale of wireless services to Mr. Shapiro, as detailed herein.

240. AT&T's acts and representations concerning the safeguards it employs to protect consumer account data—including Mr. Shapiro's data—is likely to mislead reasonable consumers, including Mr. Shapiro, as detailed herein.

241. AT&T has represented that its goods or services have characteristic and/or benefits that they do not have. Specifically, AT&T represented that, in purchasing AT&T wireless cell service and using AT&T-compatible phones, Mr. Shapiro's confidential data would be safeguarded and protected.

242. In actuality, as alleged fully above, AT&T's wireless service did not protect and/or safeguard Mr. Shapiro's data from unauthorized access, and AT&T's employees did in fact sell access to customers' personal information, as detailed herein.

243. AT&T's misrepresentations and omissions concerning its safeguarding of customers' data were materially misleading. As alleged fully above, a reasonable person would attach importance to the privacy of his sensitive account data in determining whether to contract with a wireless cell phone provider.

244. AT&T was obligated to disclose the shortcomings of its data protection practices, as AT&T had exclusive knowledge of material facts not known or knowable to its customers, AT&T actively concealed these material facts from its customers, and such disclosures were necessary to materially qualify its representations that it did not sell and took measures to protect consumer data and its partial disclosures concerning its use of customers' CPNI. Further admissions were necessary to prevent AT&T's statements from misleading the public in light of the undisclosed facts concerning its security procedures.

245. Further, AT&T was obligated to disclose its practices—by seeking consent beforehand or informing customers of breaches in the aftermath—under the FCA.

246. AT&T's actions and conduct complained of herein were a substantial factor in causing the harm suffered by Mr. Shapiro, as alleged fully above.

247. Mr. Shapiro seeks injunctive relief, damages—including actual, statutory, and punitive damages—and attorneys' fees for AT&T's violations of the CLRA. Plaintiff seeks public injunctive relief against AT&T's unfair and unlawful practices in order to protect the public and restore to the parties in interest money or property taken as a result of AT&T's unfair methods of competition and unfair

or deceptive acts or practices. Mr. Shapiro seeks a mandatory cessation of AT&T's practices and proper safeguarding of confidential customer account data.

COUNT VII
Violation of the Computer Fraud and Abuse Act
18 U.S.C. § 1030

248. Mr. Shapiro realleges and incorporates all of the preceding paragraphs as though fully set forth in this cause of action.

249. Mr. Shapiro's mobile device is capable of connecting to the Internet.

250. AT&T employees, Jack and/or White, in the scope of their employment, intentionally accessed Mr. Shapiro's mobile device, and assisted others in accessing his mobile device, without Mr. Shapiro's authorization, in order to assist hackers in their theft from Mr. Shapiro.

251. The AT&T employees, Jack and/or White, took these actions knowing that they would cause damage to Mr. Shapiro's mobile device, as well as damage to the information located on his mobile device.

252. The AT&T employees, Jack and/or White, caused Mr. Shapiro's mobile device and much of the data on it to be unusable to him.

253. Because of the AT&T employees' actions, Mr. Shapiro suffered damage to his mobile device and damage to information on his mobile device, including being unable to access information and data on his mobile device and being unable to access his personal accounts, including his personal (e.g. Evernote and G-mail) and financial (e.g. cryptocurrency and PayPal) accounts.

254. The act of swapping Mr. Shapiro's AT&T wireless SIM card was in the scope of the AT&T employees' work.

255. Further, Mr. Shapiro spent in excess of $5,000 investigating who accessed his mobile device and damaged information on it.

VII. PRAYER FOR RELIEF

256. WHEREFORE, Plaintiff Seth Shapiro requests that judgment be entered against Defendant and that the Court grant the following:

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

B. Public injunctive relief requiring cessation of Defendant's acts and practices complained of herein pursuant to, *inter alia*, Cal. Bus. & Prof. Code § 17200, 47 U.S.C. § 401(b), and Cal. Civ Code § 1780;

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

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

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

F. 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: October 15, 2019

Respectfully submitted,

Thomas D. Warren (SBN 160921)
twarren@piercebainbridge.com
Andrew Calderón (SBN 316673)
acalderon@piercebainbridge.com
PIERCE BAINBRIDGE BECK PRICE & HECHT LLP
355 S. Grand Avenue, 44th Floor,
Los Angeles, CA 90071
Telephone: (213) 262-9333
Facsimile: (213) 279-2008

Dwayne D. Sam (*pro hac application forthcoming*)
dsam@piercebainbridge.com
PIERCE BAINBRIDGE BECK PRICE & HECHT LLP
600 Pennsylvania Aveniue NW
South Tower, Suite 700
Washington, DC 20004
Telephone: (202) 843-8342
Facsimile: (202) 899-5666