PIERCE O'DONNELL (SBN 081298)
PODonnell@GreenbergGlusker.com
TIMOTHY J. TOOHEY (SBN 140117)
TToohey@GreenbergGlusker.com
PAUL BLECHNER (SBN159514)
PBlechner@GreenbergGlusker.com
GREENBERG GLUSKER FIELDS CLAMAN & MACHTINGER LLP
1900 Avenue of the Stars, 21st Floor
Los Angeles, California 90067-4590
Telephone: 310.553.3610
Fax: 310.553.0687

Attorneys for Plaintiff
MICHAEL TERPIN

UNITED STATES DISTRICT COURT

CENTRAL DISTRICT OF CALIFORNIA

MICHAEL TERPIN,

Plaintiff,

v.

AT&T INC.; AT&T Mobility, LLC; and DOES 1-25,

Defendants.

Case No. 2:18-cv-6975

COMPLAINT FOR:

(1) DECLARATORY RELIEF: UNENFORCEABILITY OF AT&T CONSUMER AGREEMENT AS UNCONSCIONABLE AND CONTRARY TO PUBLIC POLICY; (2) UNAUTHORIZED DISCLOSURE OF CUSTOMER CONFIDENTIAL PROPRIETARY INFORMATION AND PROPRIETARY NETWORK INFORMATION, FEDERAL COMMUNICATIONS ACT, 47 U.S.C. §§ 206, 222; (3) ASSISTING UNLAWFUL ACCESS TO COMPUTER, CAL. PENAL CODE § 502 ET SEQ.; (4) VIOLATION OF CALIFORNIA UNFAIR COMPETITION LAW—UNLAWFUL BUSINESS PRACTICE CAL. BUS. & PROF. CODE § 17200 ET SEQ.; (5) VIOLATION OF CALIFORNIA UNFAIR COMPETITION LAW—UNFAIR BUSINESS PRACTICE,

CAL. BUS. & PROF. CODE § 17200 ET SEQ.; (6) VIOLATION OF CALIFORNIA UNFAIR COMPETITION LAW—FRAUDULENT BUSINESS PRACTICE CAL. BUS. & PROF. CODE § 17200 ET SEQ.; (7) VIOLATION OF CALIFORNIA CONSUMER LEGAL REMEDIES ACT, CAL. CIV. CODE § 1750 ET SEQ.; (8) DECEIT BY CONCEALMENT, CAL. CIV. CODE §§ 1709, 1710; (9) MISREPRESENTATION; (10) NEGLIGENCE; (11) NEGLIGENT SUPERVISION AND TRAINING; (12) NEGLIGENT HIRING; (13) BREACH OF CONTRACT—AT&T PRIVACY POLICY; (14) BREACH OF IMPLIED CONTRACT IN THE ALTERNATIVE TO BREACH OF CONTRACT; (15) BREACH OF COVENANT OF GOOD FAITH AND FAIR DEALING; (16) VIOLATION OF CALIFORNIA CONSUMER RECORDS ACT—INADEQUATE SECURITY, CAL. CIV. CODE § 1798.81.5

DEMAND FOR JURY TRIAL

GREENBERG GLUSKER FIELDS CLAMAN & MACHTINGER LLP
1900 Avenue of the Stars, 21st Floor
Los Angeles, California 90067-4590

Plaintiff Michael Terpin, by and through his counsel, complains and alleges as follows against AT&T, Inc. and its wholly owned subsidiary AT&T Mobility, LLC (collectively, "AT&T"):

JURISDICTION AND VENUE

1. 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 matter under 28 U.S.C. § 1332 in that the amount in controversy exceeds $75,000 and Plaintiff and Defendants are citizens of different states in that Plaintiff, Michael Terpin is domiciled in Puerto Rico with a residence in California, and Defendants

AT&T, Inc. and AT&T Mobility, Inc., are corporations with their principal places of business, respectively, in Texas and Georgia.

2. Venue is proper in this Court under 28 U.S.C. §§ 1391(b)(1), (b)(2), (c) and (d) because a substantial part of the events or omissions giving rise to this Complaint occurred in this District. Plaintiff Michael Terpin has a residence in Los Angeles County, California. Mr. Terpin obtained wireless services from AT&T in Los Angeles County in or about the mid-1990's. AT&T does business in and is subject to the Court's jurisdiction in this District. AT&T's violation of Mr. Terpin's privacy in those services is the subject of this complaint. Mr. Terpin continued at all times relevant to the allegations herein to receive wireless services from AT&T for a telephone number with a Southern Californian area code.

INTRODUCTION

3. AT&T solemnly promises its cellular telephone subscribers that it will safeguard their private information—and particularly their data-rich SIM cards—from any unauthorized disclosure. Besides the numerous promises that AT&T makes in its own Privacy Policy and Code of Business Conduct, federal and state law impose a strict duty on the nation's second largest cellular telephone carrier to take all necessary steps to preserve the privacy of its almost 140 million customers. In AT&T's case, this mandate has fallen on deaf ears.

4. In one notorious instance, AT&T employees were found culpable for stealing personal information for over 200,000 customers and selling it to criminals to unlock mobile phones. This massive security failure prompted the Federal Communications Commission to levy a record fine of $25 million and secure a Consent Decree requiring AT&T to implement detailed measures to enhance its subscribers' protection against unauthorized disclosures of their private information. AT&T did not learn its lesson.

5. More recently, AT&T employees are participating in a new species of fraud—SIM swap fraud—which is a metastasizing cancer attacking

GREENBERG GLUSKER FIELDS CLAMAN & MACHTINGER LLP
1900 Avenue of the Stars, 21st Floor
Los Angeles, California 90067-4590

AT&T customers and allowing hackers readily to bypass AT&T security to rob AT&T customers of valuable personal information and millions of dollars of cryptocurrency.

6. AT&T's subscriber privacy protection system is thus a veritable modern-day Maginot Line: a lot of reassuring words that promote a false sense of security. AT&T persists in not providing adequate security even though it knows that hackers target its systems because the hackers know they are riddled with flaws. Most troubling, AT&T has not improved its protections even though it knows from numerous incidents that some of its employees actively cooperate with hackers in SIM swap frauds by giving hackers direct access to customer information and by overriding AT&T's security procedures. In recent incidents, law enforcement has even confirmed that AT&T employees profited from working directly with cyber terrorists and thieves in SIM swap frauds.

7. The porosity of AT&T's privacy program is dramatically evident in this case, which follows a pattern well known to AT&T. An experienced, high profile cryptocurrency investor, Plaintiff Michael Terpin was a longtime AT&T subscriber who entrusted his sensitive private information to AT&T and relied on AT&T's assurances and its compliance with applicable laws. Given all the carrier's hype about protecting customer security, Plaintiff believed that it would keep its promises about absolutely safeguarding him from a data breach that could lead to the theft of tens of millions of dollars of crypto currency. In reality, however, Plaintiff was victimized by not one, but two hacks within seven months.

8. Even after AT&T had placed vaunted additional protection on his account after an earlier hacking incident, an imposter posing as Mr. Terpin was able to easily obtain Mr. Terpin's telephone number from an insider cooperating with the hacker without the AT&T store employee requiring him to present valid identification or to give Mr. Terpin's required password.

GREENBERG GLUSKER FIELDS CLAMAN & MACHTINGER LLP
1900 Avenue of the Stars, 21st Floor
Los Angeles, California 90067-4590

9. The purloined telephone number was accessed to hack Mr. Terpin's accounts, resulting in the loss of nearly $24 million of cryptocurrency coins.

10. It was AT&T's act of providing hackers with access to Mr. Terpin's telephone number without adhering to its security procedures that allowed the cryptocurrency theft to occur. What AT&T did was like a hotel giving a thief with a fake ID a room key *and* a key to the room safe to steal jewelry in the safe from the rightful owner.

11. AT&T is doing nothing to protect its almost 140 million customers from SIM card fraud. AT&T is therefore directly culpable for these attacks because it is well aware that its customers are subject to SIM swap fraud and that its security measures are ineffective. AT&T does virtually nothing to protect its customers from such fraud because it has become too big to care.

12. This lawsuit seeks to hold AT&T accountable for its abject failure to protect subscribers like Mr. Terpin. Apparently, AT&T would prefer to buy Time Warner for over $85 billion than pay for a state-of-the art security system and hire, train, and supervise competent and ethical employees—even when it was well known to AT&T that its system was vulnerable to precisely the type of hack experienced by Mr. Terpin. A verdict for $24 million of compensatory damages and over $200 million for punitive damages might attract the attention of AT&T's senior management long enough to spend serious money on an acceptable customer protection program and measures to ensure that its own employees are not complicit in theft and fraud. Then and only then will AT&T's promise to protect the types of personal information that directly led to the hacking of Mr. Terpin's accounts ring true.

GREENBERG GLUSKER FIELDS CLAMAN & MACHTINGER LLP
1900 Avenue of the Stars, 21st Floor
Los Angeles, California 90067-4590

GREENBERG GLUSKER FIELDS CLAMAN & MACHTINGER LLP
1900 Avenue of the Stars, 21st Floor
Los Angeles, California 90067-4590

THE PARTIES

13. Mr. Terpin is well known for his involvement with cryptocurrency. Cryptocurrency (also known as "crypto") is digital or virtual currency designed as a medium of exchange in which encryption techniques generate units of currency that verify the transfer of funds through an encrypted ledger called "blockchain." Cryptocurrency is decentralized, operates independently of a central bank, and is often traded by parties through "exchanges." The total market value of all cryptocurrency has previously exceeded $800 billion, and there are many who project it to hit $1 trillion by the end of 2018.

14. Mr. Terpin is a prominent member of the blockchain and cryptocurrency community. In 2013, he started Bit Angels, the first angel group for investing in bitcoin companies, and CoinAgenda, the first high-end investor series for family offices and funds investing in digital assets. Mr. Terpin also runs the preeminent public relations firm in the cryptocurrency sector. Like others in the cryptocurrency community, Mr. Terpin is a high-profile hacker target because of his publicized involvement in cryptocurrency enterprises.

15. AT&T, Inc. is a Delaware Corporation with its principal place of business in Dallas, Texas. AT&T Mobility, LLC ("AT&T Mobility"), which is marketed as "AT&T," is a wholly-owned subsidiary of AT&T, Inc. with its principal place of business in Brookhaven, Georgia. AT&T Mobility provides wireless service to subscribers in the United States, Puerto Rico, and the U.S. Virgin Islands. AT&T Mobility is a "common carrier" governed by the Federal Communications Act ("FCA"), 47 U.S.C. § 151 *et seq.* AT&T Mobility is regulated by the Federal Communications Commission ("FCC") for its acts and practices, including those occurring in this District. AT&T, Inc. and AT&T Mobility are herein referred to collectively as "AT&T."

GREENBERG GLUSKER FIELDS CLAMAN & MACHTINGER LLP
1900 Avenue of the Stars, 21st Floor
Los Angeles, California 90067-4590

16. AT&T Mobility is the second largest wireless provider in the United States with 138.8 million subscribers as of the third quarter of 2017. AT&T, Inc., as it is presently constituted, is the result of the recombination of many of the companies split off from the original AT&T (also known as "The Telephone Company" or "Ma Bell.") AT&T, Inc. is a behemoth which, in 2017, had operating revenues of over $160 billion and assets of over $444 billion.

17. Over the past decade, AT&T 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 has purchased for a total equity value of $85.4 billion Time Warner Inc.—the owner of HBO, Warner Bros, CNN, Turner Broadcasting, Cartoon Network, Turner Classic Movies, TBS, TNT and Turner Sports.

18. According to media reports, AT&T mobile telephone customers have been the subject of more privacy violations than subscribers to other cell phone companies. The Electronic Frontier Foundation has recently called out AT&T's "hypocrisy" in calling for an "Internet Bill of Rights" when in fact "few companies have done more to combat privacy and network neutrality than AT&T." https://www.eff.org/deeplinks/2018/01/hypocrisy-atts-internet-bill-rights AT&T has even lobbied the FCC to stop applying the privacy provisions of the FCA to its broadband services, while arguing (unsuccessfully) that it was not subject to the jurisdiction of the Federal Trade Commission ("FTC") to govern privacy and data

GREENBERG GLUSKER FIELDS CLAMAN
& MACHTINGER LLP
1900 Avenue of the Stars, 21st Floor
Los Angeles, California 90067-4590

security pursuant to its jurisdiction to regulate unfair and deceptive acts under Section 5 of the FTC Act, 15 U.S.C. § 45(a)(1)(2).

19. As further detailed below, AT&T has also been subject to other incidents of SIM card swap fraud, including incidents involving prominent members of the cryptocurrency community. It is further aware that its employees are complicit in such fraud and can bypass AT&T's security concerns. Despite the incidents, AT&T persists in not securing its system against a cresting wave of such fraudulent activity.

20. Given AT&T's dismal track record on consumer privacy, including the FCC's fine and Consent Decree referenced below and its failure to prevent fraud of the sort that victimized Mr. Terpin, it ought to invest its money and attention to protecting its cellular telephone subscribers from the onslaught of hacking and insider data breaches before it spends billions of dollars for new companies, like Time Warner. After all, AT&T was historically a *telephone* company.

21. Plaintiff is ignorant of the true names or capacities of the defendants sued herein under the fictitious names DOES ONE through TWENTY-FIVE inclusive. Plaintiff further alleges that each of the fictitiously named Defendants is responsible in some manner for the occurrences herein alleged, proximately caused plaintiff's damages, and was acting as agent for the others.

FACTUAL ALLEGATIONS

AT&T'S STATUTORY OBLIGATION TO PROTECT CUSTOMERS' PERSONAL INFORMATION UNDER THE FEDERAL COMMUNICATIONS ACT

22. As a common carrier, AT&T is obligated to protect the confidential personal information of its customers under Section 222 of the FCA, 47 U.S.C. § 222.

GREENBERG GLUSKER FIELDS CLAMAN & MACHTINGER LLP
1900 Avenue of the Stars, 21st Floor
Los Angeles, California 90067-4590

23. Section 222(a), 47 U.S.C. § 222(a), provides that "[e]very telecommunications carrier has a duty to protect the confidentiality of proprietary information of, and relating to . . . customers . . .." The "confidential proprietary information" referred to in Section 222(a), is abbreviated herein as "CPI."

24. Section 222(c), 47 U.S.C. § 222(c), additionally provides that "[e]xcept as required by law or with the approval of the customer, a telecommunications carrier that receives or obtains customer proprietary network information by virtue of its provision of a telecommunications service shall only use, disclose, or permit access to individually identifiable customer proprietary network information in its provision of (A) the telecommunications service from which such information is derived, or (B) services necessary to, or used in, the provision of such telecommunications service, including the publishing of directories." The "customer proprietary network information" referred to in Section 222(c) is abbreviated herein as "CPNI."

25. Section 222(h)(1), 47 U.S.C. § 222(h)(1), defines CPNI as "(A) 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 (B) information contained in the bills pertaining to telephone exchange service or telephone toll service received by a customer of a carrier, except that term does not include subscriber list information."

26. The FCC has promulgated rules to implement Section 222 "to ensure that telecommunications carriers establish effective safeguards to protect against unauthorized use or disclosure of CPNI." *See* 47 CFR § 64.2001 *et seq.* ("CPNI Rules"); *CPNI Order*, 13 FCC Rcd. at 8195 ¶ 193. The CPNI Rules limit disclosure and use of CPNI without customer approval to certain limited

GREENBERG GLUSKER FIELDS CLAMAN
& MACHTINGER LLP
1900 Avenue of the Stars, 21st Floor
Los Angeles, California 90067-4590

circumstances (such as cooperation with law enforcement), none of which are applicable to the facts here. 47 CFR § 64.2005.

27. The CPNI Rules require carriers to implement safeguards to protect customers' CPNI. These safeguards include: (i) training personnel "as to when they are and are not authorized to use CPNI"; (ii) establishing "a supervisory review process regarding carrier compliance with the rules;" and (iii) filing annual compliance certificates with the FCC. 47 CFR § 64.2009(b), (d), and (e).

28. The CPNI Rules further require carriers to implement measures to prevent the disclosure of CPNI to unauthorized individuals. 47 CFR § 64.2010. For example, "carriers must take reasonable measures to discover and protect against attempts to gain unauthorized access to CPNI." 47 CFR § 64.2010(a). Moreover, "carriers must properly authenticate a customer prior to disclosing CPNI based on customer-initiated telephone contact, online account access, or an in-store visit." *Id.* In the case of in-store access to CPNI, "[a] telecommunications carrier may disclose CPNI to a customer who, at a carrier's retail location, *first presents to the telecommunications carrier or its agent a valid photo ID matching the customer's account information*." 47 CFR § 64.2010(d) (emphasis added). "Valid photo ID" is defined in 47 CFR § 64.2003(r) as "a government-issued means of personal identification with a photograph such as a driver's license, passport, or comparable ID that is not expired."

29. The FCC has determined that information obtained from customers through a common social engineering ploy known as "pretexting" is CPNI. *See In the Matter of Implementation of the Telecommunications Acts of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information*, 22 FCC Rcd. 6927 (2007) ("Pretexting Order"). 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 communications records." *Id.*, n. 1. Such "call detail" and

GREENBERG GLUSKER FIELDS CLAMAN
& MACHTINGER LLP
1900 Avenue of the Stars, 21st Floor
Los Angeles, California 90067-4590

"private communications" are CPI and CPNI under the FCA. *Id.* at 6928 *et seq.* The FCC concluded that "pretexters have been successful at gaining unauthorized access to CPNI" and that "carriers' record on protecting CPNI demonstrate[d] that the Commission must take additional steps to protect customers from carriers that have failed to adequately protect CPNI." *Id*. at 6933. The FCC modified its rules to impose additional security for carriers' disclosure of CPNI and to require that law enforcement and customers be notified of security breaches involving CPNI. *Id.* at 6936-62.

30. In its Pretexting Order, the FCC stated that it "fully expect[s] carriers to take every reasonable precaution to protect the confidentiality of proprietary or personal customer information." *Id*. at 6959, ¶ 64. The FCC further stated that "[w]e decline to immunize carriers from possible sanction for disclosing customers' private information without appropriate authorization." *Id*. at 6960, ¶ 66. In a statement directly relevant to the facts alleged below, the FCC also stressed the fact that *someone having obtained information fraudulently is strong evidence of the carrier's failure to satisfy the requirements of section 222*. The FCC stated that "we hereby put carriers on notice that the Commission henceforth will infer from evidence that a pretexter has obtained unauthorized access to a customer's CPNI that the carrier did not sufficiently protect that customer's CPNI. A carrier then must demonstrate that the steps it has taken to protect CPNI from unauthorized disclosure, including the carrier's policies and procedures, are reasonable *in light of the threat posed* by pretexting and the *sensitivity of the customer information at issue*." *Id*. at 6959, ¶ 63 (emphasis added).

31. As further alleged below, AT&T violated Section 222 of the FCA and the CPNI Rules and ignored the warning in the Pretexting Order on January 7, 2018 when its employees provided hackers with Mr. Terpin's SIM cards containing or allowing access to Mr. Terpin's personal information, including CPI and CPNI, without Mr. Terpin's authorization or permission, and without requiring

that the individual accessing Mr. Terpin's account present valid identification or comply with AT&T's own procedures.

AT&T EMPLOYEES' DISCLOSURE OF CUSTOMERS' PERSONAL INFORMATION AND THE APRIL 8, 2015 FCC CONSENT DECREE

32. On April 8, 2015, the FCC fined AT&T a record $25 million for violating Section 222 of the FCA by allowing its employees to hand over to thieves the CPNI of almost 280,000 customers. In addition to being forced to pay $25 million to the FCC, AT&T entered into a consent decree requiring it to implement measures to protect CPNI. The April 8, 2015 consent decree ("Consent Decree") remains in full force and effect.

33. In the Consent Decree and the FCC's adopting order ("Adopting Order"), the FCC highlights AT&T's lax security practices and dismal failure to supervise and monitor employees that led to its unprecedented breach of its customers' confidential and private information. *See In the Matter of AT&T Services, Inc.*, 30 FCC Rcd. 2808 (April 8, 2015 Adopting Order and Consent Decree) (attached hereto as Exhibit A).

34. The FCC investigation revealed that numerous AT&T call center employees provided the CPNI of hundreds of thousands of customers, including names, phone numbers and Social Security Numbers to unauthorized third parties, who used this information to gain access to unlock codes for mobile telephones and to remove territorial and network restrictions. *Id*. at 2808. The investigation further revealed that employees were frequently paid by criminals to hand over AT&T customers' personal sensitive information, including account-related CPNI. *Id*. at 2808, 2813-15.

35. The FCC found that AT&T employees used their login credentials to access the confidential information of almost 280,000 customers. The FCC concluded that AT&T's data security measures "failed to prevent or timely detect a large and ongoing Data Breach." *Id.* at 2813 (Consent Decree ¶ 8).

GREENBERG GLUSKER FIELDS CLAMAN & MACHTINGER LLP
1900 Avenue of the Stars, 21st Floor
Los Angeles, California 90067-4590

GREENBERG GLUSKER FIELDS CLAMAN
& MACHTINGER LLP
1900 Avenue of the Stars, 21st Floor
Los Angeles, California 90067-4590

36. The FCC also found that AT&T had not properly supervised its employees' access to its customers' personal information, including CPNI. 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 constitutes an unjust and unreasonable practice in violation of the Act." *Id. at* 2808 (Adopting Order § 2).

37. In the Adopting Order, the FCC emphasized the importance of AT&T's obligation to adhere to the obligations embodied in Section 222 of the FCA. According to the Adopting Order, the purpose of Section 222 is 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." *Id*. Carriers like AT&T are thus required to take "'every reasonable precaution' to protect their customers' data" and to notify consumers regarding any breaches in order to "aid in the pursuit and apprehension of bad actors and provide valuable information that helps affected consumers [to] be proactive in protecting themselves in the aftermath of a data breach." *Id*.

38. As a condition of terminating the FCC's investigation of AT&T's violations of Sections 201(b) and 222 of the FCA, the FCC imposed numerous requirements on AT&T to improve its supervision of employees and to adhere to its legal obligation to protect the privacy of AT&T's customers. Moreover, the Consent Decree imposed obligations not only on AT&T itself, but also on AT&T's "Covered Employees," who are defined as "all employees and agents of AT&T who perform or directly supervise, oversee, or manage the performance of duties that involve access to, use, or disclosure of Personal Information or Customer Proprietary Network Information at Call Centers managed and operated by AT&T Mobility." *Id.* at 2811. "Call Center" is defined broadly in the Consent Decree as call centers operated by AT&T or its contractors "that

provide mobility customer service or wireless sale service for AT&T Mobility consumer customers." *Id*. at 2810.

39. Paragraph 17 of the FCC Consent Decree requires AT&T to designate "a senior corporate manager with the requisite corporate and organization authority to serve as a Compliance Officer . . .." *Id*. at 2816. AT&T's Compliance Officer must be "responsible for developing, implementing, and administering the Compliance Plan and ensuring that AT&T complies with the terms and conditions of the Compliance Plan and this Consent Decree." *Id*.

40. Paragraph 18 of the FCC Consent Decree requires AT&T to institute a "Compliance Plan designed to ensure future compliance with the [FCA] and with the terms and conditions of this Consent Decree." *Id.* The Compliance Plan must include a Risk Assessment, Information Security Program, Ongoing Monitoring and Improvement, and a Compliance Review. *Id.*

41. The "Information Security Program" required in Paragraph 18(b) must be "reasonably designed to protect CPNI and Personal Information from unauthorized access, use, or disclosure by Covered Employees . . .." *Id.* AT&T's program must be documented in writing and include:

> (i) administrative, technical, and physical safeguards reasonably designed to protect the security and confidentiality of Personal Information and CPNI;
>
> (ii) reasonable measures to protect Personal Information and CPNI maintained by or made available to Vendors, Covered Employees, and Covered Vendor Employees. . .;
>
> (iii) access controls reasonably designed to limit access to Personal Information and CPNI to authorized AT&T employees, agents, and Covered Vendor Employees;
>
> (iv) reasonable processes to assist AT&T in detecting and responding to suspicious or anomalous account activity, including whether by

GREENBERG GLUSKER FIELDS CLAMAN & MACHTINGER LLP
1900 Avenue of the Stars, 21st Floor
Los Angeles, California 90067-4590

malware or otherwise, involving Covered Employees and Covered Vendor Employees; and

(v) a comprehensive breach response plan that will enable AT&T to fulfill its obligations under applicable laws, with regard to breach notifications, including its obligations under paragraph 20 while that paragraph remains in effect.

42. Paragraph 18(c) of the Consent Decree requires AT&T to "monitor its Information Security Program on an ongoing basis to ensure that it is operating in a manner reasonably calculated to control the risks identified through the Risk Assessment, to identify and respond to emerging risks or threats, and to comply with the requirements of Section 222 of the [FCA], the CPNI Rules, and this Consent Decree." *Id.* at 2817. In addition, Paragraph 18(g) requires AT&T to "establish and implement a Compliance Training Program [for employees] on compliance with Section 222, the CPNI Rules, and the Operating Procedures." *Id.* All "Covered Employees" are required to be trained within six months of hire and periodically thereafter. *Id.*

43. AT&T must report noncompliance with the terms and conditions of the Consent Decree within fifteen (15) days after discovery of such noncompliance. *Id.* at 2819 (Consent Decree ¶ 20). In addition, "AT&T shall also report to the FCC any breaches of Personal Information or CPNI involving any Covered Employees or Covered Vendor Employees that AT&T is required by any federal or state law to report to any Federal or state entity or any individual." *Id.* Moreover, AT&T is required to file compliance reports with the FCC six (6) months after the Effective Date, twelve (12) months after the Effective Date, and thirty-six (36) months after the Effective Date." *Id.* (Consent Decree ¶ 21).

44. The provisions in Paragraphs 17 and 18 of the Consent Decree were applicable at all relevant dates to the acts and omissions alleged in this Complaint. *Id.* at 2820 (Consent Decree ¶ 22 (Paragraphs 17-18 expire seven (7)

GREENBERG GLUSKER FIELDS CLAMAN & MACHTINGER LLP
1900 Avenue of the Stars, 21st Floor
Los Angeles, California 90067-4590

GREENBERG GLUSKER FIELDS CLAMAN & MACHTINGER LLP
1900 Avenue of the Stars, 21st Floor
Los Angeles, California 90067-4590

years after the "Effective Date," *i.e.*, April 7, 2022)). As further alleged below, AT&T violated numerous terms of the April 8, 2015 Consent Decree by failing to implement adequate security procedures to protect Mr. Terpin's personal information, including CPNI, by failing to supervise and monitor its employees, by failing to ensure that its employees were ethical and competent, by failing to follow its security procedures and by failing to follow its legal obligations to protect Mr. Terpin's personal information under the FAC, CPNI Rules, and the Consent Decree. Mr. Terpin alleges on information and belief that AT&T also failed to report to the FCC the two data breaches involving Mr. Terpin, as required by FCC regulations and the Consent Decree. Mr. Terpin further alleges on information and belief that AT&T has failed to report to the FCC additional data breaches involving victims of fraud where AT&T employees provided hackers access AT&T's customers' telephone numbers who stole money from the customers.

AT&T'S PRIVACY AND SECURITY COMMITMENTS TO CUSTOMERS IN ITS PRIVACY POLICY AND CODE OF BUSINESS CONDUCT

45. In its Privacy Policy ("Privacy Policy") and Code of Business Conduct ("COBC"), AT&T acknowledges its responsibilities to protect customers' "Personal Information" under the FCA, the CPNI Rules and other regulations. A true and correct copy of the Privacy Policy in effect in January 2018 available at http://about.att.com/sites/privacy_policy is attached hereto as Exhibit B. A true and correct copy of the COBC in effect in January 2018 available at https://ebiznet.sbc.com/attcode/index.cfm is attached hereto as Exhibit C.

46. In its Privacy Policy and COBC, AT&T makes binding promises and commitments to Mr. Terpin, as its customer, that it will protect and secure his "Personal Information." The Privacy Policy defines "Personal Information" as "[i]nformation that identifies or reasonably can be used to figure out the identity of a customer or user, such as your name, address, phone number and e-mail address." AT&T states that, among the information that it collects from

and about its customers, are "your name, address, telephone number, e-mail address" and service-related details such as payment history, security codes, service history and similar information. AT&T also collects information relating to the use of its networks, products and services. "Personal Information" thus includes both CPI and CPNI under Section 222 of the FCA and the CPNI Rules.

47. In its Privacy Policy AT&T promises that it takes its responsibility "to safeguard your [*i.e.*, the customer's] Personal Information seriously" and that it will not share its customers' Personal Information except for legitimate business purposes. It further states that "we will not sell [users'] Personal Information to anyone, for any purpose. Period."

48. AT&T further promises that it has numerous safeguards in place to protect the Personal Information of its customers and makes the following promises to its customers:

> We've worked hard to protect your information. *And we've established electronic and administrative safeguards designed to make the information we collect secure*. Some examples of those safeguards include:
>
> - All of our employees are subject to the AT&T Code of Business Conduct (COBC) **(**https://www.att.com/Common/about_us/downloads/att_code_of_business_conduct.pdf**)** and certain state-mandated codes of conduct. Under the COBC, all employees must follow the laws, rules, regulations, court and/or administrative orders that apply to our business—including, specifically, the legal requirements and company policies surrounding the privacy of communications and the security and privacy of your records. We take this seriously, and any of our employees who fail to meet the standards we've set in the COBC are subject to disciplinary action. That includes dismissal.

GREENBERG GLUSKER FIELDS CLAMAN & MACHTINGER LLP
1900 Avenue of the Stars, 21st Floor
Los Angeles, California 90067-4590

GREENBERG GLUSKER FIELDS CLAMAN & MACHTINGER LLP
1900 Avenue of the Stars, 21st Floor
Los Angeles, California 90067-4590

- We've implemented technology and security features and strict policy guidelines to safeguard the privacy of your Personal information. Some examples are:
  - Maintaining and protecting the security of computer storage and network equipment, and using our security procedures that require employee user names and passwords to access sensitive data;
  - Applying encryption or other appropriate security controls to protect Personal Information when stored or transmitted by us;
  - Limiting access to Personal Information to only those with jobs requiring such access; and
  - *Requiring caller/online authentication before providing Account Information so that only you or someone who knows your Account Information will be able to access or change this information.*

(Emphasis added.)

49. AT&T's COBC also makes binding commitments to Mr. Terpin, as an AT&T customer, that it will protect his Personal Information and that it will adhere to all its legal obligations. Those legal obligations include, by implication, Section 222 of the FCA, the CPNI Rules, and other legal obligations that govern protection of confidential and private information. For example, AT&T's chairman and chief executive, Randall Stephenson, and its chief compliance officer, David Huntley promise that because "[o]ur customers count on us" "[t]hat we will follow not only the letter of the law, but the spirit of the law" and "that we will always take responsibility." *The COBC also specifically promises that AT&T will "protect the privacy of our customers' communications" because "[n]ot only do our customers demand this, but the law requires it.*

GREENBERG GLUSKER FIELDS CLAMAN & MACHTINGER LLP
1900 Avenue of the Stars, 21st Floor
Los Angeles, California 90067-4590

Maintaining the confidentiality of communication is, and always has been, a crucial part of our business." (Emphasis added.)

50. AT&T further promises in the COBC that it "protect[s] the information about our customers that they entrust to us." Acknowledging that "AT&T possesses sensitive, detailed information about our customers, who rely on AT&T to safeguard that information" and that "[l]aws and regulations tell us how to treat such data," AT&T promises Mr. Terpin, as an AT&T customer, that "[a]ny inappropriate use of confidential customer information violates our customers' trust and may also violate a law or regulation. *Preserving our customers' trust by safeguarding their private data is essential to our reputation.*" (Emphasis added.)

51. As alleged below, AT&T flagrantly and repeatedly violated its commitments to Mr. Terpin in its Privacy Policy and COBC, as well as its legal obligations under the FCA, the CPNI Rules, the Consent Decree, and California law, by willingly turning over to hackers Mr. Terpin's wireless number that allowed hackers to access his "Personal Information" including CPNI. AT&T's betrayal of its obligations caused Mr. Terpin to lose nearly $24 million worth of cryptocurrency.

THE PREVALENCE OF SIM CARD SWAP FRAUD

52. AT&T is directly liable for the harm suffered by Mr. Terpin because it has long known that its customers are subject to SIM swap fraud (also called SIM swapping, SIM hijacking, or "port out scam") perpetrated by hackers often with the active cooperation of its own employees. The prevalence of such fraud is established by numerous news reports, the experience of other AT&T customers known to Plaintiff, and Mr. Terpin's own doleful experience.

53. As described in in a July 30, 2018 article in *Motherboard* entitled "'Tell Your Dad to Give Us Bitcoin:' How a Hacker Allegedly Stole Millions by Hijacking Phone Numbers," available at https://motherboard.vice.com/en_us/article/a3q7mz/hacker-allegedly-stole-

millions-bitcoin-sim-swapping "SIM swapping consists of tricking a provider like AT&T or T-Mobile into transferring the target's phone number to a SIM card controlled by the criminal. Once they get the phone number, fraudsters can leverage it to reset the victims' passwords and break into their online accounts (cryptocurrency accounts are common targets.) In some cases, this works even if the accounts are protected by two-factor authentication. This kind of attack, also known as 'port out scam,' is relatively easy to pull off and has become widespread, as a recent Motherboard investigation showed."

54. The leading security reporter Brian Krebs wrote on August 18, 2018 (https://krebsonsecurity.com/2018/08/florida-man-arrested-in-sim-swap-conspiracy/) that "SIM swaps are frequently abused by scam artists who trick mobile providers into tying a target's service to a new SIM card and mobile phone that the attackers control. Unauthorized SIM swaps often are perpetrated by fraudsters who have already stolen or phished a target's password, as many banks and online services rely on text messages to send users a one-time code that needs to be entered in addition to a password for online authentication." As Mr. Krebs also wrote: "[i]n some cases, fraudulent SIM swaps succeed thanks to lax authentication procedures at mobile phone stores. *In other instances, mobile store employees work directly with cyber criminals to help conduct unauthorized SIM swaps. . . .*" (Emphasis added.)

55. Mr. Terpin alleges on information and belief that AT&T knew well before the attacks on Mr. Terpin that it was subject to widespread SIM swap fraud. Mr. Terpin alleges further that AT&T knew that cryptocurrency investors like Plaintiff were specifically targeted by SIM swapping and that AT&T was the weak link in such fraud. This is confirmed in numerous articles on SIM swap fraud, including that of Brian Krebs and a July 31, 2018 article in bitcoinist.com entitled "Sim-Swapping Bitcoin Thief Charged in California Court," available at https://bitcoinist.com/sim-swapping-bitcoin-thief-charged-california-court/. The

GREENBERG GLUSKER FIELDS CLAMAN & MACHTINGER LLP
1900 Avenue of the Stars, 21st Floor
Los Angeles, California 90067-4590

bitcoinist.com article states that "the liability for [SIM swapping] attacks [lies] squarely at the feet of the service providers [which the article calls the 'weakest link'] as security procedures for confirming identity should not be bypass-able using a few pieces of personal information easily obtained online."

56. Mr. Terpin also alleges on information and belief that AT&T knew or should have known that its employees frequently cooperated with hackers and thieves to bypass its security procedures. This is confirmed not only by Brian Krebs, who wrote that "mobile store employees work directly with cyber criminals," but in an August 3, 2018 article in *Motherboard* entitled "How Criminals Recruit Telecom Employees to Help them Hijack SIM Cards," available at https://motherboard.vice.com/en_us/article/3ky5a5/criminals-recruit-telecom-employees-sim-swapping-port-out-scam, which describes how scammers routinely recruit and pay employees of AT&T and other Telecoms called "plugs" to perform illegal SIM swaps.

57. Mr. Terpin further alleges on information and belief that despite its knowledge that its employees actively cooperate with hackers to rob its own customers, AT&T has done nothing to prevent such scams. As an AT&T employee confirmed in the August 3, 2018 *Motherboard* article, "if a criminal finds a corrupt insider, 'there aren't enough safeguards [in place] to stop that employee,' . . .." The AT&T employee further told the author of the article that "*the system is designed so that some employees have the ability to override security features such as the phone passcode that AT&T (and other companies) now require when porting numbers*. 'From there the passcode can be changed,' the employee said in an online chat, referring to a customer information portal that they showed *Motherboard*. 'With a fresh passcode the number can be ported out with no hang ups.'" (Emphasis added.)

58. Mr. Terpin alleges on information and belief that countless AT&T customers have been the victims of SIM swapping and that those customers

GREENBERG GLUSKER FIELDS CLAMAN & MACHTINGER LLP
1900 Avenue of the Stars, 21st Floor
Los Angeles, California 90067-4590

have lost hundreds of millions of dollars or more because of the fraud. This is confirmed by the July 30, 2018 *Motherboard* article, which describes the arrest of Joel Ortiz, one of a group of criminals from Boston, who "used the increasingly popular technique known as SIM swapping or SIM hijacking to steal bitcoin, other cryptocurrencies and social media accounts." In a fraud that mirrors the one suffered by Mr. Terpin some months earlier, Ortiz "*specifically targeted people involved in the world of cryptocurrency and blockchain*," including in an incident where he *stole more than $1.5 million from a cryptocurrency entrepreneur who was an AT&T customer*." (Emphasis added)

59. This is further confirmed in the August 18, 2018 article by Brian Krebs, which describes the arrest of Ricky Joseph Handschumacher in Florida, who was charged with grand theft and money laundering for draining cryptocurrency accounts through SIM fraud. According to Krebs, Handschumacher's group came to light "when a Michigan woman called police after she overheard her son talking on the phone and pretending to be an AT&T employee. Officers responding to the report searched the residence and found multiple cell phones and SIM cards, as well as files on the kid's computer that included 'an extensive list of names and phone numbers of people from around the world.'"

60. Krebs' report further revealed that "[t]he Pasco County [Florida] Sheriff's office says their surveillance of the Discord [voice chat] server revealed that the group *routinely paid employees at cellular phone companies to assist in their attacks, and that they even discussed a plan to hack accounts belonging to the CEO of cryptocurrency exchange Gemini Trust Company*." (Emphasis added.)

61. Mr. Terpin alleges on information and belief that AT&T is fully aware of these and numerous other SIM swapping incidents involving its customers, including incidents where its own employees were complicit with hackers. For example, the *Motherboard* article confirms that AT&T had provided investigators with the victim's call records "for the days when the hacker was

GREENBERG GLUSKER FIELDS CLAMAN & MACHTINGER LLP
1900 Avenue of the Stars, 21st Floor
Los Angeles, California 90067-4590

allegedly in control of the investor's numbers." Indeed, those records were used by law enforcement in issuing a warrant for e-mails from the phone which produced incriminating evidence against Ortiz.

62. Mr. Terpin further alleges on information and believe that federal enforcement agencies have compiled proof that insiders at AT&T cooperated in SIM swap fraud that was directed at members of the cryptocurrency community. Mr. Terpin further alleges that such insiders actively cooperated with hackers to provide them customer list information.

63. The prevalence of SIM swap fraud and AT&T's knowledge of such fraud, including the active participation of its own employees in the fraud, demonstrate that the January 7, 2018 SIM swap fraud on Mr. Terpin that led to the theft of nearly $24 million in cryptocurrency was neither an isolated nor an unforeseeable event.

THE JUNE 11, 2017 HACK

64. On or about June 11, 2017, Mr. Terpin discovered that his AT&T cell phone number had been hacked when his phone suddenly became inoperable. As Mr. Terpin learned from AT&T a few days later, his AT&T password had been changed remotely after 11 attempts in AT&T stores had failed. By obtaining control over Mr. Terpin's phone, the hackers diverted Mr. Terpin's personal information, including telephone calls and text messages, to get access to accounts that use telephone numbers as a means of verification or authentication.

65. After the hackers took charge of Mr. Terpin's telephone number, the hackers accessed Mr. Terpin's telephone to divert texts and telephone calls to gain access to Mr. Terpin's cryptocurrency accounts. The hackers also used the phone to hijack Mr. Terpin's Skype account to impersonate him. By that means, the hackers convinced a client of Mr. Terpin to send them cryptocurrency and diverted a payment due to Mr. Terpin to themselves. AT&T finally cut off access

GREENBERG GLUSKER FIELDS CLAMAN & MACHTINGER LLP
1900 Avenue of the Stars, 21st Floor
Los Angeles, California 90067-4590

by the hackers to Mr. Terpin's telephone number on June 11, 2017, but only after the hackers had stolen substantial funds from Mr. Terpin. Moreover, because of the hack, Mr. Terpin expended a substantial amount of time investigating the hack and attempting to repair his computer accounts.

66. On or about June 13, 2017, Mr. Terpin met with AT&T representatives in Puerto Rico to discuss the June 11, 2017 hack. Mr. Terpin explained to AT&T that he had been hacked and that the hackers had stolen a substantial amount of money from him. Mr. Terpin expressed concern about AT&T's ineffective security protections and asked how he could protect the security of his phone number and account against future unauthorized access, including hackers attempting to perpetrate SIM swap fraud.

67. In response to Mr. Terpin's request for greater security for his account, AT&T promised that it would place his account on a "higher security level" with "special protection." AT&T told Mr. Terpin that this "higher security level" would require anyone accessing or changing Mr. Terpin's account to provide a six-digit passcode to AT&T to access or change the account. Anyone requesting AT&T to transfer Mr. Terpin's telephone number to another phone must provide the code. AT&T promised Mr. Terpin at this meeting that the higher security that it was placing on his account, which it also called "high risk" or "celebrity" protection, would insure that Mr. Terpin's account was much less likely to be subject to SIM swap fraud. AT&T further told Mr. Terpin that the implementation of the increased security measures would prevent Mr. Terpin's number from being moved to another phone without Mr. Terpin's explicit permission, because no one other than Mr. Terpin and his wife would know the secret code.

68. At alleged above, AT&T was well aware at the time of the June 11, 2017 incident that its users were subject to SIM swap fraud. It was also well aware that its employees cooperated in such fraud and that the employees could bypass its security procedures. Mr. Terpin alleges on information and belief that

GREENBERG GLUSKER FIELDS CLAMAN & MACHTINGER LLP
1900 Avenue of the Stars, 21st Floor
Los Angeles, California 90067-4590

GREENBERG GLUSKER FIELDS CLAMAN
& MACHTINGER LLP
1900 Avenue of the Stars, 21st Floor
Los Angeles, California 90067-4590

AT&T had been previously contacted numerous times by law enforcement authorities about such frauds involving its own employees who actively cooperated with hackers. Nonetheless, AT&T recommended that customers who were concerned about fraudulent actions on their account add purported "extra security" by adding a "wireless security password" to protect their account. AT&T touted the benefits of such "extra" security on its website because it would require a password for "*managing your account in any retail store.*" *See* https://www.att.com/esupport/article.html#!/wireless/KM1051397 (emphasis added).

69. Mr. Terpin relied upon AT&T's promises that his account would be much more secure against hacking, including SIM swap fraud, after it implemented the increased security measures. Because of the implementation of such measures, Mr. Terpin retained his account with AT&T. But for these express promises and assurances, Mr. Terpin would have canceled his AT&T account and contracted with a different cellular telephone provider and he would not have lost nearly $24 million from hackers.

70. Mr. Terpin further alleges on information and belief that AT&T knew at the time that it recommended that he adopt additional security on his account that the additional security measures were not adequate and could be overridden by its employees. In reality, the vaunted extra protection was, like the Maginot Line, a useless defense that was easily evaded by AT&T's own employees, who it knew or should have known actively cooperated with hackers in SIM swap fraud. Despite AT&T's knowledge of the futility of these actions, AT&T falsely informed Mr. Terpin, to his detriment, that he should implement such additional security measures.

THE JANUARY 7, 2018 SIM SWAP FRAUD

71. AT&T's promises proved to be false and the increased security illusory. On Sunday January 7, 2018, an employee in an AT&T store cooperated

with an imposter committing SIM swap fraud. Unbeknownst to Mr. Terpin, AT&T had grossly misrepresented its ability to secure Mr. Terpin's Personal Information after the June 11, 2017 incident. Not only had AT&T failed to disclose that it did not properly supervise, train or monitor its employees to ensure that they scrupulously followed AT&T's security procedures, but it also failed to disclose that it knew that its employees could readily bypass the higher security protection placed on Mr. Terpin's account after the June 11, 2017 hack.

72. On January 7, 2018, Mr. Terpin's phone with his AT&T wireless number went dead. Mr. Terpin was again a victim of SIM swap fraud. As AT&T later admitted, an employee in an AT&T store in Norwich, Connecticut ported over Mr. Terpin's wireless number to an imposter in violation of AT&T's commitments and promises, including the higher security that it had supposedly placed on Mr. Terpin's account after the June 11, 2017 hack that had supposedly been implemented to prevent precisely such fraud. Through the January 7, 2018 hack, thieves gained control over Mr. Terpin's accounts and stole nearly $24 million worth of cryptocurrency from him on January 7 and 8, 2018.

73. When Mr. Terpin's telephone went dead on January 7, 2018, he instantly attempted to contact AT&T to have the telephone number immediately canceled so that the hackers would not gain access to his Personal Information and accounts. Ignoring Mr. Terpin's urgent request, AT&T failed promptly to cancel Mr. Terpin's account, which gave the hackers sufficient time to obtain information about Mr. Terpin's cryptocurrency holdings and to spirit off funds to their own accounts. Adding insult to injury, AT&T placed Mr. Terpin's wife on endless hold (over an hour!) when she asked to be connected to AT&T's fraud department while Mr. Terpin was furiously attempting to see what damage was being done to his accounts. Mr. Terpin's wife never reached AT&T's fraud department because it apparently does not work (or is unavailable) on Sundays. But the hackers work on Sunday!

GREENBERG GLUSKER FIELDS CLAMAN & MACHTINGER LLP
1900 Avenue of the Stars, 21st Floor
Los Angeles, California 90067-4590

74. The employees at the AT&T store who unlawfully handed over Mr. Terpin's telephone number to thieves were either blind or complicit. It was impossible to look at Mr. Terpin's account information on the AT&T computer screen and not see the multiple warnings about the need for heightened vigilance, particularly the requirement of a six-digit password. Nonetheless, as AT&T had reason to know before the January 7, 2018 incident (but had never informed Mr. Terpin or other customers), its employees could readily bypass its much-touted security procedures.

75. In cooperating willingly with hackers committing SIM swap fraud to plunder Mr. Terpin's accounts, AT&T violated its own policies as well as the requirements of Section 222 of the FCA and the FCC Consent Decree. On information and belief, AT&T knew that its employees were frequently complicit with SIM swap frauds and could readily bypass its security procedures. Mr. Terpin further alleges that AT&T did not even attempt to require the hacker to provide the six-digit code that AT&T required for access to Mr. Terpin's "high profile" account or to require a supervisor to approve the manual override. Indeed, AT&T admitted to Mr. Terpin on February 4, 2018 that a sales associate in AT&T's Norwich, Connecticut location had violated AT&T's procedures by not only failing to ask for the six-digit code, but also by bypassing its requirement that the hacker have a scannable ID to obtain a replacement SIM card for Mr. Terpin's wireless number. On information and belief, Mr. Terpin alleges that the employee in the AT&T store who handed over the SIM card to the imposter had a criminal record and was cooperating with the hacker and that AT&T had failed properly to supervise the employee, despite its knowledge that its employees cooperated in precisely this type of fraud.

76. Because of AT&T's cooperation and failure to follow its own policies, the hackers were able to intercept Mr. Terpin's personal information,

GREENBERG GLUSKER FIELDS CLAMAN & MACHTINGER LLP
1900 Avenue of the Stars, 21st Floor
Los Angeles, California 90067-4590

GREENBERG GLUSKER FIELDS CLAMAN
& MACHTINGER LLP
1900 Avenue of the Stars, 21st Floor
Los Angeles, California 90067-4590

including telephone calls and text messages, and gain access to his cryptocurrency accounts.

77. Because of AT&T's willing cooperation with the hacker, gross negligence, violation of its statutory duties, and failure to adhere to its commitments in its Privacy Policy and COBC, as well as its obligations under the FCC Consent Degree and its commitments to Mr. Terpin after the June 11, 2017 hack, Mr. Terpin lost nearly $24 million worth of cryptocurrency.

78. To Mr. Terpin's knowledge, AT&T never informed either the FCC, the FBI or any other law enforcement or regulatory authority about the January 7, 2018 SIM swap. Nor did AT&T ever provide Mr. Terpin with a written explanation of how the SIM swap fraud occurred or a claim form, let alone an apology for facilitating the hack. In contrast, Mr. Terpin himself reported the January 7, 2018 SIM swap to the FBI and the Secret Service Cyber Crimes Unit and has actively sought an investigation of the hack and recovery of the stolen funds. To date, Mr. Terpin has not been able to recover any of the funds that were stolen.

79. On information, Mr. Terpin alleges that AT&T did not discipline or terminate the employee who turned over a SIM card for his telephone number to imposters and who facilitated the theft of nearly $24 million worth of Mr. Terpin's cryptocurrency.

FIRST CLAIM FOR RELIEF

(Declaratory Relief:

Unenforceability of AT&T Consumer Agreement as Unconscionable and Contrary to Public Policy)

80. Mr. Terpin brings this claim for declaratory relief under 28 U.S.C. § 2201 to have the Court declare that AT&T's wireless customer agreement (the "Agreement") is unconscionable, void against public policy under Cal. Civ. Code §§ 1670.5 and 1668, and unenforceable in its entirety.

GREENBERG GLUSKER FIELDS CLAMAN & MACHTINGER LLP
1900 Avenue of the Stars, 21st Floor
Los Angeles, California 90067-4590

81. Mr. Terpin initially entered into a wireless contract with AT&T in or about 2011 when he transferred the account from his wife. Mr. Terpin has asked AT&T for a copy of his agreement, but AT&T refused to provide it to him. Mr. Terpin thus has no copy of any agreement with AT&T for wireless services.

82. The agreement was presented to Mr. Terpin, like all other wireless users, on a take-it-or-leave-it basis. Mr. Terpin had no ability to negotiate any term of the agreement. In contrast, AT&T has virtually unlimited power over its customers, including Mr. Terpin, as seen below by the fact that it purports to hold Mr. Terpin and all other wireless users to the terms of an agreement that they may well have never seen or read.

83. The version of the Agreement posted in early 2018 purports to govern AT&T's provision of wireless service to all customers, including Mr. Terpin who first contracted with AT&T over two decades ago. A true and correct copy of the Agreement posted on AT&T's website in early 2018 at https://www.att.com/legal/terms.wirelessCustomerAgreement-list.html is attached hereto as Exhibit D. As alleged below, the Agreement contains numerous unconscionable terms that renders it unenforceable in its entirety because its "central purpose . . . is tainted with illegality." *Ingle v. Circuit City Stores, Inc.*, 328 F.3d 1165, 1180 (9th Cir. 2003) (holding invalid an agreement that obstructs the ability of customers to bring any claims against defendant).

84. The Agreement states that the Agreement and other agreements that are "not otherwise described below that are posted on applicable AT&T websites or devices, and any documents expressly referred to herein or therein, make up the complete agreement between you and AT&T and supersede any and all prior agreements and understandings relating to the subject matter of this Agreement." Through such vague language, AT&T apparently contends that not only the Agreement, but other unspecified and unknown agreements, bind all wireless customers, whether or not such customers have seen the Agreement or are

aware of its terms. In other words, every time AT&T mints a new (and more onerous) version of its agreements, its unsuspecting customers are purportedly bound by the new terms. This practice highlights the fact that not only are these contracts not negotiable, they are invisible. What you don't see, you still get.

85. The Agreement is a classic contract of adhesion imposed by AT&T upon a party with no bargaining power. In contrast, AT&T has unchecked power to insist upon its own terms even if the consumer is unaware of the terms of the Agreement itself. There is no ability to negotiate any term of the Agreement. It is literally "take it or leave it."

86. The Agreement is void as against public policy under Cal. Civ. Code § 1668 as a contract of adhesion purporting to bind customers who have never heard or seen the agreement and most likely are entirely unaware of its provisions. The Agreement is void and unenforceable in its entirety because it also contains exculpatory provisions, damage waivers, and an indemnification provision that purport to prevent consumers from bringing *any* claims against AT&T or obtaining redress for their claims -- even for billing errors.

87. The exculpatory provision in Paragraph 4.1 of the Agreement ("Exculpatory Provision") contains numerous provisions that are contrary to public policy under Cal. Civ. Code § 1668 because they attempt to exempt AT&T from responsibility for its own gross negligence, fraud, and violations of law. In pertinent part, the Exculpatory Provision states that:

> ***WE DO NOT GUARANTEE YOU UNINTERRUPTED SERVICE OR COVERAGE.*** . . . AT&T MAKES NO WARRANTY, EXPRESS OR IMPLIED, OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE, SUITABILITY, ACCURACY, ***SECURITY OR PERFORMANCE REGARDING ANY SERVICES, SOFTWARE OR GOODS, AND IN NO EVENT SHALL AT&T BE***

GREENBERG GLUSKER FIELDS CLAMAN & MACHTINGER LLP
1900 Avenue of the Stars, 21st Floor
Los Angeles, California 90067-4590

LIABLE, WHETHER OR NOT DUE TO ITS OWN NEGLIGENCE, for any:

a. act or omission of a third party;

b. mistakes, omissions, interruptions, errors, failures to transmit, delays, or defects in the Services or Software provided by or through us;

c. ***damages or injury caused by the use of Services, Software, or Device***, including use in a vehicle . . ..

(Capitalization in original; emphasis added in bold and italics.)

88. The Exculpatory Provision renders the entire Agreement unenforceable on public policy grounds under Cal. Civil Code §§ 1668 and 1670.5 because it purports to exempt AT&T from its gross negligence, statutory violations and willful behavior, including the egregious conduct alleged herein. The Exculpatory Provision is further against public policy because it purports to exempt AT&T from violation of statutory obligations, including the obligation to maintain the confidentiality and security of its customers' private and personal information under Section 222 of the FCA, the FCC Consent Degree, and numerous provisions of California State law, including California unfair competition law, the Consumer Legal Remedies Act, and the California Customer Records Act. Thus, even where, as here, AT&T willfully violates its statutory duties under the FCA and the Consent Decree, not to mention its promises in its Privacy Policy and the COBC, a customer is prevented by the Exculpatory Provision from bringing a claim for negligent or willful disclosure of the customer's Personal Information, including CPNI, because such claim seeks redress for "damages or injury caused by the use of Services, Software, or Device . . ." and is waived by the Exculpatory Provision.

89. AT&T also seeks in the contract to have customers waive any damages, except for providing a "credit equal to a pro-rata adjustment of the

GREENBERG GLUSKER FIELDS CLAMAN & MACHTINGER LLP
1900 Avenue of the Stars, 21st Floor
Los Angeles, California 90067-4590

monthly Services fee for the time period your Services was unavailable, not to exceed the monthly Service fee" when a customer's services are interrupted.

90. Section 4.1 of the Agreement ("Damages Restriction") is also void under Cal. Civ. Code §§ 1668 and 1670.5 because it purports to exempt AT&T for all other damages:

> Unless prohibited by law, AT&T isn't liable for any indirect, special, punitive, incidental or consequential losses or damages you or any third party may suffer by use of, or inability to use, Services, Software or Devices provided by or through AT&T, including loss of business or goodwill, revenue or profits, or claims of personal injuries.

91. The Exculpatory Provision is invalid under Civil Code § 1670.5 because it allocates all the risks to the consumer with AT&T disclaiming any damages for its own conduct—even fraud, gross negligence, and statutory violations, including those governed by the FCA. Thus, even if AT&T deliberately handed over a customer's CPNI to hackers in violation of Section 222 of the FCA, a customer would not be entitled to the full range of damages afforded by that statute under the Damages Restriction.

92. The Damages Restriction included in a contract of adhesion as to which AT&T's users, including Mr. Terpin, have no bargaining authority, is void because it is plainly unconscionable and against public policy. The Damages Restriction is contained in a lengthy form contract drafted by a domineering telecommunication provider with vast assets in a far superior bargaining position to the wireless user. Indeed, it is no exaggeration to say that the consumer has no bargaining power as regards AT&T, particularly as to the Damages Restriction and other draconian provisions in the Agreement. Because the Damages Restriction is found in a document posted on a website that, by fiat, is automatically made applicable to customers, customers may not even be aware that they have virtually no redress against AT&T, unless they diligently monitor changes in the website.

GREENBERG GLUSKER FIELDS CLAMAN & MACHTINGER LLP
1900 Avenue of the Stars, 21st Floor
Los Angeles, California 90067-4590

Moreover, the Damages Restriction is contained in a complex and lengthy contract that provides essential wireless services—without which most customers have no means of communication (including for emergency services), let alone essential computing, geolocation, texting, research or other services.

93. The Damages Restriction is also substantively unconscionable because it allocates risks in an objectively unreasonable manner. *See Armendariz v. Foundation Health Psychcare Services, Inc.*, 24 Cal. 4th 83, 113-114 (2000). The allocation of risks under the Agreement is objectively unreasonable because AT&T—a telecommunications behemoth with billions of dollars of assets and tens of millions of customers—takes upon itself virtually no liability (other than minimal recompense for interrupted services) and purports to exempt itself from virtually all damages, including those arising out of its own deliberate, grossly negligent, or fraudulent acts.

94. The Agreement is further unenforceable because customers are purportedly required to indemnify AT&T for all claims arising out of the services provided by AT&T, including claims that arise due to AT&T's negligence, gross negligence, deliberate conduct, or statutory violations. The indemnity provision in Paragraph 4.1 of the Agreement ("Indemnity") states:

> To the full extent allowed by law, you hereby release, indemnify, and hold AT&T and its officers, directors, employees and agents harmless from and against *any and all claims of any person or entity for damages of any nature arising in any way from or relating to, directly or indirectly, service provided by AT&T* or any person's use thereof (including, but not limited to vehicular damage and personal injury), *INCLUDING CLAIMS ARISING IN WHOLE OR IN PART FROM THE ALLEGED NEGLIGENCE OF AT&T*, or any violation by you of this Agreement.

(Capitalization in original; emphasis added.)

GREENBERG GLUSKER FIELDS CLAMAN & MACHTINGER LLP
1900 Avenue of the Stars, 21st Floor
Los Angeles, California 90067-4590

95. Read literally, the Indemnity requires a consumer, such as Mr. Terpin, to hold AT&T harmless for AT&T's own negligence, deliberate behavior, gross negligence, statutory violations (including disclosure of CPNI under the FCA), or fraud if the conduct is related "directly or indirectly" to any "service provided by AT&T." On its face, the indemnity provision in a contract of adhesion renders the entire Agreement unconscionable and unenforceable because if defeats the entire purpose of the contract by making it impossible for consumers to bring claims against AT&T for the entire range of statutory rights to which a consumer, such as Mr. Terpin, is entitled. Indeed, the Indemnity would totally obviate AT&T's commitment to privacy in its Privacy Policy as well as its legal obligations under the FCA, the CPNI Rules, and the Consent Decree.

96. Because the entire Agreement is unenforceable because the central purpose of the Agreement is "tainted with illegality . . . [so that] the contract as a whole cannot be enforced," the arbitration provision in Paragraph 2.2 of the Agreement ("Arbitration Provision") is also enforceable. *See, Armendariz,* 24 Cal. 4th at 89-90.

97. The Arbitration Provision would require Mr. Terpin to arbitrate his claims "without affording the full range of statutory remedies, including punitive damages and attorney fees" that are available to him under the claims alleged herein. *Armendariz*, 24 Cal. 4th at 103 (damages limitation unlawful if applied to statutory claims). For example, Mr. Terpin, if required to arbitrate this claim, would be forced by the Damages Limitation to forego his statutory entitlement to punitive damages under his Third Claim for Relief under California Penal Code § 502 *et seq.* and to his entitlement to punitive damages for AT&T's fraud and negligence. Moreover, the Arbitration Provision would require Mr. Terpin to forego the full range of damages to which he is entitled under his Second Claim for Relief under the Federal Communications Act § 222. These defects

GREENBERG GLUSKER FIELDS CLAMAN & MACHTINGER LLP
1900 Avenue of the Stars, 21st Floor
Los Angeles, California 90067-4590

render not only the Arbitration Provision, but also the entire Agreement, unenforceable.

98. Because the defenses raised by Mr. Terpin as to the unconscionability of the Agreement are "enforced evenhandedly" and do not "interfere[] with the fundamental attributes of arbitration," they do not run afoul of *AT&T Mobility LLC v. Concepcion*, 563 U.S. 333 (2010). The Court's decision in *Concepcion* did not abrogate the savings clause of the FAA that provides that arbitration agreements may be declared unenforceable "upon such grounds as exist at law or in equity for the revocation of any contract," including "generally applicable contract defenses, such as fraud, duress, or unconscionability." *Concepcion* at 339, *quoting* 9 U.S.C. § 2 and *Doctors Associates, Inc. v. Casarotto*, 517 U.S. 681, 687 (1996). For the reasons alleged in this claim, such defenses apply squarely to the Agreement.

99. There is an actionable and justiciable controversy between Mr. Terpin and AT&T in that Mr. Terpin contends that the Agreement, including the Exculpatory Provision, Damages Restriction, Indemnity and Arbitration Provision, is unenforceable in its entirety because it is unconscionable and void against public policy since it prevents consumers, such as Mr. Terpin, from obtaining redress against AT&T even for deliberate acts in violation of its legal duties. AT&T undoubtedly disagrees.

100. A judicial declaration of the enforceability of the Agreement, including the Exculpatory Provision, Damages Restriction, Indemnity and Arbitration Provision and all other provisions of the Agreement, is necessary and appropriate.

101. Mr. Terpin seeks a judgment declaring that the Agreement in its entirety is unenforceable as unconscionable and against public or, in the alternative that (a) the Exculpatory Provision is unenforceable as against Mr. Terpin; (b) the Damages Restriction is unenforceable against Mr. Terpin; (c) the Indemnity is

GREENBERG GLUSKER FIELDS CLAMAN & MACHTINGER LLP
1900 Avenue of the Stars, 21st Floor
Los Angeles, California 90067-4590

unenforceable as against Mr. Terpin; and (d) the Arbitration Provision is unenforceable as against Mr. Terpin

SECOND CLAIM FOR RELIEF

(Unauthorized Disclosure of Customer Confidential Proprietary Information and Proprietary Network Information

(Federal Communications Act, 47 U.S.C. §§ 206, 222))

102. Plaintiff realleges the allegations in Paragraphs 1-101 as if fully set forth herein.

103. AT&T is a "common carrier" engaging in interstate commerce by wire regulated by the Federal Communications Act ("FCA") and subject to the requirements, *inter alia*, of sections 206 and 222 of the FCA.

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

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

106. Section 222(c)(1) of the FCA, 27 U.S.C. § 222(c)(1) further requires that, "[e]xcept as required by law or with the approval of the customer, a telecommunications carrier that receives or obtains customer proprietary information by virtue of its provision of a telecommunications service shall only use, disclose, or permit access to customer proprietary network information

GREENBERG GLUSKER FIELDS CLAMAN & MACHTINGER LLP
1900 Avenue of the Stars, 21st Floor
Los Angeles, California 90067-4590

GREENBERG GLUSKER FIELDS CLAMAN
& MACHTINGER LLP
1900 Avenue of the Stars, 21st Floor
Los Angeles, California 90067-4590

['CPNI'] in its provision of (A) telecommunications services from which such information is derived, or (B) services necessary to or used in the provision of such telecommunication services. . .."

107. The information disclosed to hackers by AT&T in the January 7, 2018 SIM swap fraud transferring Mr. Terpin's telephone number, was CPI and CPNI under Section 222 of the FCA.

108. AT&T failed to protect the confidentiality of Mr. Terpin's CPI and CPNI, including his wireless telephone number, account information, and his private communications, by divulging that information to hackers in the January 7, 2018 SIM swap fraud. Through its negligence, gross negligence and deliberate acts, including inexplicable failures to follow its own security procedures, supervise its employees, the CPNI Regulations, the terms of the Consent Decree, the warnings of the Pretexting Order, its Privacy Policy and the COBC, and by allowing its employees to bypass such procedures, AT&T permitted hackers to access Mr. Terpin's telephone number, telephone calls, text messages and account information to steal nearly $24,000,000 worth of his cryptocurrency.

109. As a direct consequence of AT&T's violations of the FCA, Mr. Terpin has been damaged by loss of nearly $24,000,000 worth in cryptocurrency which AT&T allowed to fall into the hands of thieves, and for other damages in an amount to be proven at trial.

110. Mr. Terpin is also entitled to his attorney's fees under the FCA in bringing this action against AT&T for its gross negligence and fraudulent misrepresentation as to the security that it provides for customer accounts as required by the FCA, the CPNI Regulation, and the Consent Decree.

GREENBERG GLUSKER FIELDS CLAMAN
& MACHTINGER LLP
1900 Avenue of the Stars, 21st Floor
Los Angeles, California 90067-4590

THIRD CLAIM FOR RELIEF

(Assisting Unlawful Access to Computer

California Penal Code § 502 *et seq.*)

111. Mr. Terpin realleges the allegations in Paragraphs 1-110 as if fully set forth herein.

112. AT&T violated California Penal Code § 502 *et seq.* by knowingly and without permission allowing unauthorized third parties to access Mr. Terpin's computers, computer systems and computer networks, including his mobile phone.

113. As herein alleged, AT&T on or about January 7, 2018 transferred Mr. Terpin's telephone number to unauthorized individuals who used it to access his computer systems and accounts.

114. When AT&T handed over Mr. Terpin's wireless number and account to unauthorized individuals, AT&T was on notice that Mr. Terpin's Personal Information was vulnerable to attack because it was aware of the prevalence of SIM swap fraud, pretexting scams, and its employees' misconduct, including as detailed in the Consent Decree. AT&T was also aware that Mr. Terpin was vulnerable because he had contacted AT&T after the June 11, 2017 incident and AT&T had placed additional "high security" safeguards on Mr. Terpin's account to guard against potential future attacks. In addition to other mandated procedures, these safeguards included requiring anyone who wished to access Mr. Terpin's account in an AT&T store to provide a six-digit passcode.

115. Although AT&T was aware of the necessity for safeguards for its customers' Personal Information under the FCA, CPNI Rules, and the Consent Decree, and had made specific commitments to Mr. Terpin after the June 11, 2017 incident that it was placing additional security on Mr. Terpin's accounts, AT&T on January 7, 2018 did not require the unauthorized individual to provide it with the required six-digit passcode or legally proper identification and allowed its

GREENBERG GLUSKER FIELDS CLAMAN
& MACHTINGER LLP
1900 Avenue of the Stars, 21st Floor
Los Angeles, California 90067-4590

employee to bypass the protections on Mr. Terpin's account. Instead, AT&T cooperated with the hackers by porting over Mr. Terpin's wireless number to telephones controlled by hackers that then allowed them to access Mr. Terpin's Personal Information, including CPNI.

116. AT&T's blatant disregard of its high security procedures and willing cooperation with the hackers on January 7, 2018 constitutes knowing cooperation with unauthorized individuals accessing Mr. Terpin's computers, computer systems, and computer networks. AT&T knew from the June 11, 2017 incident that Mr. Terpin was a high-profile target and that hackers had accessed Mr. Terpin's computers, computer systems, and computer networks. Mr. Terpin further alleges on information and belief that it knew that individuals in the crypto currency community were particularly subject to SIM swap fraud and that its employees actively cooperated with such hackers to victimize its own customers.

117. AT&T further knew that the hackers to whom it ported Mr. Terpin's telephone number on January 7, 2018 were not authorized to access Mr. Terpin's Personal Information because the hackers did not have identification conforming to AT&T's or the FCC's requirements under the CPNI Rule. Indeed, on January 7, 2018 AT&T handed over Mr. Terpin's telephone number and Personal Information even though the hackers further lacked the required "high security" six-digit code required to access or modify Mr. Terpin's wireless account.

118. Because of AT&T's knowing cooperation with the hackers in the January 7, 2018 SIM swap fraud, AT&T provided the hackers with means to access Mr. Terpin's computers, computer systems, and computer networks and to steal nearly $24 million worth of cryptocurrency from Mr. Terpin.

119. What is truly mystifying here is how the hacker for the January 7, 2018 crime could get Mr. Terpin's telephone number on the first try. Back on July 11, 2017, the criminals were unable to get the number even though they visited *11 stores*. Most likely, as AT&T knew, the January 7, 2018 hacker was an inside

job facilitated by a "plug" employee at the AT&T facility! Either way, AT&T is left holding the bag.

120. Because of the conduct alleged herein by AT&T, Mr. Terpin is entitled to compensatory damages and injunctive relief under Penal Code § 502(e)(1). Mr. Terpin is also entitled to reasonable attorney fees pursuant to Penal Code § 502(e)(2).

121. Because AT&T's conduct as alleged herein is willful and was conducted with oppression, fraud or malice as defined in Civil Code § 3294(c), Mr. Terpin is entitled to punitive or exemplary damages in an amount to be proven at trial.

FOURTH CLAIM FOR RELIEF

(Violation of California Unfair Competition Law

Unlawful Business Practice

Cal. Bus. & Prof. Code § 17200 *et seq.*)

122. Plaintiff realleges the allegations in Paragraphs 1-121 as if fully stated herein.

123. Because of the conduct alleged herein, AT&T engaged in unlawful practices within the meaning of the California Unfair Competition Law ("UCL"), Cal. Bus. & Prof. Code § 17200 *et seq*. The conduct alleged herein is a "business practice" within the meaning of the UCL.

124. AT&T stored and processed Mr. Terpin's Personal Information, including CPI and CPNI, in its electronic systems and databases. Mr. Terpin's CPNI and other Personal Information could readily be accessed when Mr. Terpin's telephone number was ported out to a new telephone controlled by a hacker. All such information is "Personal Information" under AT&T's Privacy Policy.

125. AT&T falsely represented to Mr. Terpin and other customers in its Privacy Policy and COBC: (a) that its system was secure and that it would respect the privacy of its customers' information; (b) that it had "established

GREENBERG GLUSKER FIELDS CLAMAN & MACHTINGER LLP
1900 Avenue of the Stars, 21st Floor
Los Angeles, California 90067-4590

GREENBERG GLUSKER FIELDS CLAMAN & MACHTINGER LLP
1900 Avenue of the Stars, 21st Floor
Los Angeles, California 90067-4590

electronic and administrative safeguards designed to make the information we collect secure," as well as requiring employees to adhere to the COBC and other codes of conduct, including "the legal requirements and company policies surrounding the privacy of communications and the security and privacy of your records"; and (c) that it had "implemented technology and security features and strict policy guidelines to safeguard the privacy of your Personal information," including "[l]imiting access to Personal Information to only those with jobs requiring such access" and "[r]equiring caller/online authentication before providing Account Information so that only you or someone who knows your Account Information will be able to access or change this information." These security measures and safeguards included those mandated by the CPNI Rules and Consent Decree.

126. AT&T knew or should have known that it did not employ reasonable, industry standard and appropriate security measures that complied with "legal requirements," in the FCA, CPNI Rules, Consent Decree and other laws and regulations. AT&T also knew from the FCC investigation leading to the Consent Decree that its employee monitoring and training was inadequate.

127. AT&T misrepresented to Mr. Terpin after the June 11, 2017 incident that it had added "special protection" to protect Mr. Terpin's "celebrity" or "high profile" account. These increased security measures included requiring a six-digit passcode to ensure that Mr. Terpin's account would not readily be hacked, including by someone spoofing his identity and attempting to transfer his telephone number to their phone. In fact, AT&T's representations were false because an imposter was readily able to obtain Mr. Terpin's wireless number from a cooperative (or wantonly incompetent) employee at an AT&T facility on January 7, 2018 without having either proper identification or being asked to provide the required six-digit passcode.

GREENBERG GLUSKER FIELDS CLAMAN & MACHTINGER LLP
1900 Avenue of the Stars, 21st Floor
Los Angeles, California 90067-4590

128. Even without AT&T's misrepresentations after the June 11, 2017 hack, Mr. Terpin was entitled to assume that AT&T would take appropriate measures to keep secure his Personal Information, including CPI and CPNI, because of its statements in its Privacy Policy and COBC. AT&T did not disclose at any time that Mr. Terpin's CPI and CPNI were vulnerable to hackers because AT&T's security measures were ineffective. AT&T, which was the only party in possession of material information as to its own practices, did not disclose the rampant defects in its security procedures, including the ability of its employees to bypass such procedures, when it had a duty to do so. AT&T further violated the UCL by failing to implement reasonable and appropriate security measures for Mr. Terpin's Personal Information, as required by the FCA, the CPNI Rules, the Consent Decree and California law, or following industry standards for data security, and failing to comply with its own Privacy Policy and COBC. If AT&T had complied with these legal requirements, Mr. Terpin would not have suffered the damages related to the January 7, 2018 SIM swap fraud.

129. AT&T's acts, omissions, and misrepresentations as alleged herein were unlawful and in violation of, *inter alia*, the FCA, 47 U.S.C. §§ 206 and 222, the CPNI Rules, the Consent Decree, Cal. Civ. Code § 1798.81.5(b), Section 5(a) of the Federal Trade Commission Act, 15 U.S.C. § 45(a), Cal. Bus. & Prof. Code § 22576 (because of AT&T failing to comply with its own posted privacy policies), and the Consumer Legal Remedies Act, Cal. Civ. Code § 1750 *et seq.*

130. Mr. Terpin suffered injury in fact and loss money or property, including stolen crypto currencies worth nearly $24 million, as the result of AT&T's unlawful business practices. Mr. Terpin has lost the benefit of his bargain for his purchased services from AT&T that he would not have paid if he had known the truth regarding AT&T's inadequate data security.

131. Because of AT&T's unlawful business practices and violation of the UCL, Mr. Terpin is entitled to restitution, disgorgement of wrongfully obtained profits, and injunctive relief.

FIFTH CLAIM FOR RELIEF

(Violation of California Unfair Competition Law

Unfair Business Practice

Cal. Bus. & Prof. Code § 17200 *et seq.*)

132. Plaintiff realleges the allegations in Paragraphs 1-131 as if fully stated herein.

133. Because of the conduct alleged herein, AT&T engaged in unfair business practices within the meaning of the UCL.

134. AT&T stored and processed Mr. Terpin's Personal Information, including CPI and CPNI, in its electronic system and databases. Mr. Terpin's Personal Information was readily accessed when a hacker through SIM swap fraud gained access to Mr. Terpin's telephone number. AT&T represented to Mr. Terpin through its Privacy Policy and COBC that its systems and databases were secure and that his Personal Information would remain private and secure and would not be divulged to unauthorized third parties. AT&T engaged in unfair acts and business practices by representing in its Privacy Policy that it had "established electronic and administrative safeguards designed to make the information we collect secure." AT&T further represented that all its employees followed the COBC and that such employees "must follow the laws, rules, regulations, court and/or administrative orders that apply to our business—including, specifically, the legal requirements and company policies surrounding the privacy of communications and the security and privacy of your [i.e., the customer's] records."

135. AT&T further assured Mr. Terpin, after the June 11, 2017 hack, that his Personal Information, including CPI and CPNI, was secure because AT&T

GREENBERG GLUSKER FIELDS CLAMAN & MACHTINGER LLP
1900 Avenue of the Stars, 21st Floor
Los Angeles, California 90067-4590

had implemented additional security protections on his account, which it called a "higher security level" or "special", "high risk," or "celebrity" protection.

136. Even without these misrepresentations, Mr. Terpin was entitled to, and did, assume AT&T would take appropriate measures to keep his Personal Information safe under the FCA, the CPNI Rules, the Consent Decree and other laws and regulations. AT&T did not disclose at any time that Mr. Terpin's Personal Information was vulnerable to hackers by employees' turning over his telephone number that included and allowed access to his Personal Information. AT&T also did not disclose that its security measures were inadequate and outdated, its employees were not properly trained, that its employees could readily bypass its security procedures, and that it did not properly vet its employees to ensure that they were ethical and did not have a criminal record.

137. AT&T knew or should have known that it did not employ reasonable security and lacked adequate employee training and monitoring measures that would have kept Mr. Terpin's personal and financial information secure and prevented the loss or misuse of Mr. Terpin's Personal information. AT&T had been put on notice through the Consent Decree and by the June 11, 2017 hack of its lax security practices and inadequate training and supervision of employees. AT&T's system is less secure than the access portals for numerous gyms, which require fingerprint identification for entrance.

138. AT&T violated the UCL by misrepresenting, both by affirmative conduct and by omission, the security of its systems and services, and its ability to safeguard Mr. Terpin's Personal Information, including CPI and CPNI. AT&T also violated the UCL by failing to implement and maintain reasonable security procedures and practices appropriate to protect Mr. Terpin's Personal Information under the FCA, CPNI Rules, and Consent Decree, including CPI and CPNI. If AT&T had followed the industry standards and legal requirements, Mr. Terpin would not have suffered the damages related to the January 7, 2018 SIM

GREENBERG GLUSKER FIELDS CLAMAN & MACHTINGER LLP
1900 Avenue of the Stars, 21st Floor
Los Angeles, California 90067-4590

swap fraud. Moreover, if AT&T had followed the higher security measures it purportedly employed after the June 11, 2017 hack, Mr. Terpin would hot have suffered the damages from the January 7, 2018 SIM swap fraud.

139. AT&T also violated its commitment to maintain the confidentiality and security of Mr. Terpin's Personal Information, including CPI and CPNI, and failed to comply with its own policies and applicable laws, regulations, including the FCA, CPNI Rules, and the Consent Decree, and industry standards relating to data security.

140. The harm caused by AT&T's actions and omissions, as described in detail in this Complaint, greatly outweighs any perceived utility. Indeed, AT&T's failure to follow data security protocols, its own policies, and its misrepresentations to Mr. Terpin had no utility at all.

141. AT&T's actions and omissions, as described above, violated fundamental public policies expressed by the United States and California. *See, e.g.*, FCA, 47 U.S.C. § 222; CPNI Rules; Consent Decree; Cal. Civ. Code § 1798.1 ("The [California] Legislature declares that . . . all individuals have a right of privacy in information pertaining to them . . .. The increasing use of computers . . . has greatly magnified the potential risk to individual privacy that can occur from the maintenance of personal information); Cal. Civ. Code § 1798.81.5(a) ("It is the intent of the Legislature to ensure that personal information about California residents is protected."); Cal. Bus. & Prof. Code § 22578 ("It is the intent of the Legislature that this chapter [including the Online Privacy Protection Act] is a matter of statewide concern.) Defendants' acts and omission, and the injuries caused by them, are thus "comparable to or the same as a violation of law. . .." *Cel-Tech Communications, Inc. v. Los Angeles Cellular Telephone Co.*, 20 Cal. 4th 163, 187 (1999).

142. The harm caused by AT&T's actions and omissions, as described in detail above, is substantial in that it has caused Mr. Terpin to suffer

GREENBERG GLUSKER FIELDS CLAMAN & MACHTINGER LLP
1900 Avenue of the Stars, 21st Floor
Los Angeles, California 90067-4590

nearly $24 million in actual financial harm because of AT&T's unfair business practices.

143. Because of AT&T's unfair business practices and violations of the UCL, Mr. Terpin is entitled to restitution, disgorgement of wrongfully obtained profits and injunctive relief.

SIXTH CLAIM FOR RELIEF

(Violation of California Unfair Competition Law

Fraudulent Business Practice

Cal. Bus. & Prof. Code § 17200, *et seq.*)

144. Mr. Terpin realleges the allegations of Paragraphs 1-143 as if fully set forth herein.

145. Because of the conduct alleged herein, AT&T engaged in fraudulent business practices within the meaning of the UCL.

146. AT&T affirmatively represented to Mr. Terpin that his Personal Information, including CPI and CPNI, was secure and that it would remain private. AT&T engaged in fraudulent acts and business practices by misleadingly misrepresenting in its Privacy Policy that it "worked hard to protect your information" and had "established electronic and administrative safeguards designed to make the information we collect secure." AT&T further misrepresented that these safeguards included making employees subject to the COBC so that they had to "follow the laws, rules, regulations, court and/or administrative orders that apply to our business—including, specifically, the legal requirements and company policies surrounding the privacy of your records." COBC. AT&T also misrepresented that it took protecting the security of its customers' Personal Information "seriously" and that employees violating the COBC were "subject to disciplinary action," including dismissal. *Id.*

147. AT&T's misrepresentations and fraudulent conduct were particularly egregious because AT&T was subject to the Consent Decree that

GREENBERG GLUSKER FIELDS CLAMAN & MACHTINGER LLP
1900 Avenue of the Stars, 21st Floor
Los Angeles, California 90067-4590

required it, in the light of numerous violations by its employees of their obligation to protect customers' Personal Information, including CPNI, to strengthen the training and supervision of its employees.

148. AT&T further misrepresented in the COBC that it had "implemented technology and security features and strict policy guidelines to safeguard the privacy of your Personal Information" that included limiting access to Personal Information and requiring authentication before providing Account Information to authorized individuals. After the June 11, 2017 hack, AT&T also misrepresented to Mr. Terpin it was placing a higher level of security protection on the Personal Information of his "high risk" or "celebrity" account so that a six-digit code was required to modify his account, including transferring his telephone number to another phone.

149. AT&T not only made affirmative misrepresentations, but also made fraudulent omissions by concealing the true facts from Mr. Terpin. AT&T did not disclose to Mr. Terpin that its data security measures were woefully substandard, that its employees could bypass its security measures, and that it did not adequately supervise or monitor its employees so that they would adhere to the commitments it made in the Privacy Policy and the COBC, as well as the requirements of the FCA, CPNI Rules and Consent Decree.

150. AT&T's representations that it would secure the Personal Information of Mr. Terpin were facts that reasonable persons could be expected to rely upon when deciding whether to use (or continue to use) AT&T's services.

151. Mr. Terpin relied upon the representations that AT&T made after the June 11, 2017 hack and in the Privacy Policy and COBC. Based on the representations that AT&T was implementing a higher level of security, Mr. Terpin was entitled to, and did, assume AT&T would take appropriate measures to keep his Personal Information safe, including not handing over his wireless number that would allow thieves to access such information. AT&T did not disclose that the

GREENBERG GLUSKER FIELDS CLAMAN & MACHTINGER LLP
1900 Avenue of the Stars, 21st Floor
Los Angeles, California 90067-4590

higher level of security was ineffective, and that Mr. Terpin's Personal Information was vulnerable to hackers because AT&T did not follow its own procedures or monitor its employees' implementation of the procedures, as required by the FCA, CPNI Rules, and the Consent Decree.

152. Had Mr. Terpin known that AT&T's "heightened security" was ineffective and that its representations about such security were false and he had known that AT&T failed to disclose to him that its data security practices were substandard and ineffective, he would not have continued to provide his Personal Information to AT&T and continued their services.

153. Mr. Terpin suffered injury and lost money when AT&T ported over his wireless telephone number to a hacker's phone that allowed the hacker to steal nearly $24 million worth of cryptocurrency.

154. Because of AT&T's fraudulent business practices and violations of the UCL, Mr. Terpin is entitled to restitution, disgorgement of wrongfully obtained profits and injunctive relief.

SEVENTH CLAIM FOR RELIEF

(Violation of California Consumer Legal Remedies Act ("CLRA")

Cal. Civ. Code § 1750 *et seq.*)

155. Mr. Terpin realleges the allegations of Paragraphs 1 through 154 as if fully set forth herein.

156. The CLRA was enacted to protect consumers against unfair and deceptive business practices. It extends to transactions that are intended to result, or which have resulted, in the sale of goods or services to consumers. AT&T is subject to the CLRA because it provided paid wireless services to Mr. Terpin and AT&T's acts, omissions, representations and practices fall within the CLRA.

157. Mr. Terpin is a consumer within the meaning of Cal. Civ. Code § 1761(d).

GREENBERG GLUSKER FIELDS CLAMAN & MACHTINGER LLP
1900 Avenue of the Stars, 21st Floor
Los Angeles, California 90067-4590

158. AT&T's acts, omissions, misrepresentations, and practices were and are likely to deceive consumers. By misrepresenting the safety and security of its protection of Personal Information, including CPI and CPNI, AT&T violated the CLRA. AT&T had exclusive knowledge of undisclosed material facts, namely, that its protection of Personal Information was defective, and withheld that information from Mr. Terpin.

159. AT&T's acts, omissions and practices alleged herein violated the CLRA, which provides, in relevant part, that: "(a) The following unfair methods of competition and unfair or deceptive acts or practices undertaken by any person in a transaction intended to result or which results in the sale or lease of goods or services to any consumer are unlawful . . .; (5) Representing that goods or services have sponsorship, approval, characteristics, ingredients, uses, benefits, or quantities which they do not have . . . ; (7) Representing that goods or services are of a particular standard, quality, or grade . . . if they are of another. . . ; (14) Representing that a transaction confers or involves rights, remedies, or obligations which it does not have or involve, or which are prohibited by law. . . ; (16) Representing that the subject of a transaction has been supplied in accordance with a previous representation when it has not."

160. AT&T stored and processed Mr. Terpin's Personal Information, including CPI and CPNI, on its systems and databases. AT&T represented to Mr. Terpin that his Personal Information was secure and would remain private. AT&T engaged in deceptive acts and business practices by the statements that it made in the Privacy Policy and COBC that users' Personal Information was secure and that it adhered to its legal obligations to protect Personal Information, including under the FCA, CPNI Rules and the Consent Decree.

161. AT&T knew or should have known that it did not employ reasonable measures to keep Mr. Terpin's Personal Information secure and prevent the loss or misuse of that information. In fact, AT&T did not adhere to its legal

GREENBERG GLUSKER FIELDS CLAMAN & MACHTINGER LLP
1900 Avenue of the Stars, 21st Floor
Los Angeles, California 90067-4590

obligations to protect Personal Information, including those under the FCA, CPNI Rules and the Consent Decree.

162. AT&T's deceptive acts and business practices, including the commitment it made after the June 11, 2017 hack to implement a higher level of security for Mr. Terpin's Personal Information and account, induced Mr. Terpin to entrust AT&T with his Personal Information and continue to subscribe to its wireless services. But for AT&T's deceptive acts and business practices, Mr. Terpin would not have continued to provide AT&T with its Personal Information and continue to subscribe to its wireless services.

163. Mr. Terpin was harmed as the result of AT&T's violations of the CLRA because his Personal Information was compromised by divulging it to hackers without his consent which led to the loss of nearly $24 million worth of cryptocurrency through the January 7, 2018 SIM swap fraud.

164. Because of AT&T's violation of the CLRA, Mr. Terpin is entitled to compensatory and exemplary damages, an order enjoining AT&T from continuing the unlawful practices described herein, a declaration that AT&T's conduct violated the CLRA, attorneys' fees, and the costs of litigation.

EIGHTH CLAIM FOR RELIEF

(Deceit by Concealment—Cal. Civ. Code §§ 1709, 1710)

165. Mr. Terpin realleges the allegations of Paragraphs 1-164 as if fully set forth herein.

166. As alleged above, AT&T knew that its data security measures were grossly inadequate, that its employees could readily bypass the procedures, that its employees actively cooperated with hackers and thieves, and that it was incapable of living up to its commitments to consumers, including to Mr. Terpin, under state and federal law, as well as under its own Privacy Policy, to protect his Personal Information, including CPI and CPNI.

GREENBERG GLUSKER FIELDS CLAMAN & MACHTINGER LLP
1900 Avenue of the Stars, 21st Floor
Los Angeles, California 90067-4590

GREENBERG GLUSKER FIELDS CLAMAN
& MACHTINGER LLP
1900 Avenue of the Stars, 21st Floor
Los Angeles, California 90067-4590

167. As further alleged above, AT&T knew from prior incidents and contacts with law enforcement that its system was subject to SIM swap fraud, that its employees cooperated with hackers in such fraud, and that such fraud was prevalent in the cryptocurrency community.

168. In response to these facts, AT&T chose to do nothing to protect Mr. Terpin.

169. AT&T had an obligation to disclose to Mr. Terpin that his Personal Information, including CPI and CPNI, was readily obtained by hackers and that its own employees handed such information to hackers, and yet did not implement measures to protect Mr. Terpin or willfully failed to adhere to any measures that were in place, including its so-called "higher security level" for high profile or celebrity accounts and its required security and training measures under the Consent Decree. AT&T's so-called security system more resembles a thin slice of swiss cheese than a sophisticated network of "heightened security."

170. AT&T did not disclose these things to Mr. Terpin and willfully deceived Mr. Terpin by concealing the true facts concerning its data security, which AT&T was legally obligated and had a duty to disclose. It is far easier to penetrate AT&T's system than obtaining a new password from Walmart.

171. Had AT&T disclosed the true facts about its dangerously poor data security practices and its inadequate supervision and training of its employees, Mr. Terpin would have taken further measures to protect himself. Mr. Terpin justifiably relied on AT&T's statements, including statements after the June 11, 2017 hack, and further relied on AT&T to provide accurate and complete information about its data security.

172. Rather than disclosing the inadequacies in its security, AT&T willfully suppressed any information relating to such inadequacies.

173. AT&T's actions are "deceit" under Cal. Civ. Code § 1710 in that they are the suppression of a fact by one who is bound to disclose it, or who

gives information of other facts which are likely to mislead for want of communication of that fact.

174. Because of the deceit by AT&T, it is liable under Cal. Civ. Code § 1709 for "any damage which [Mr. Terpin] thereby suffers."

175. Because of this deceit by Defendants, Mr. Terpin's Personal Information, including his CPI and CPNI, was compromised by hackers and he was deprived of nearly $24 million worth of cryptocurrency. In addition, Mr. Terpin's Personal Information is now easily available to hackers, including through the Dark Web. Mr. Terpin is further damaged to the extent of the amounts that he has paid AT&T for wireless services, because those services were either worth nothing or worth less than was paid for them because of lack of security. Mr. Terpin has also suffered substantial out-of-pocket costs because of AT&T's inadequate security.

176. Because AT&T's deceit is fraud under Civil Code § 3294(c)(3), and AT&T's conduct was done with malice, fraud and oppression, Mr. Terpin is entitled to punitive damages under Civil Code § 3294(a).

NINTH CLAIM FOR RELIEF

(Misrepresentation)

177. Mr. Terpin realleges Paragraphs 1 through 176 as if fully set forth herein.

178. As outlined above, AT&T made numerous representations and false promises in its Privacy Policies and COBC as well as in its advertising, regarding the supposed security of consumers' Personal Information, including Mr. Terpin's Personal Information, and when an AT&T employee persuaded Mr. Terpin not to cancel his service after the June 11, 2017 hack. Such representations and promises were false because AT&T was using outdated security procedures and failed to disclose that it did not adhere to its own standards, including the heightened security standards that it implemented for Mr. Terpin after the June 11, 2017 hack, the CPNI Rules or the procedures mandated by the Consent Decree.

GREENBERG GLUSKER FIELDS CLAMAN & MACHTINGER LLP
1900 Avenue of the Stars, 21st Floor
Los Angeles, California 90067-4590

GREENBERG GLUSKER FIELDS CLAMAN & MACHTINGER LLP
1900 Avenue of the Stars, 21st Floor
Los Angeles, California 90067-4590

179. AT&T's misrepresentations and false promises, including those made after the June 11, 2017 hack, were material to Mr. Terpin who reasonably relied upon the representations and promises. Mr. Terpin would not have agreed to continue to use and pay for AT&T's services if he had known that they were not as secure as represented by AT&T and would not have lost nearly $24 million.

180. AT&T intended that Mr. Terpin rely on their representations and promises, including those made after the June 11, 2017 hack, as it knew that Mr. Terpin would not entrust his Personal Information to unreasonable security risks, particularly because Mr. Terpin had been subject to the June 11, 2017 hack. In reliance upon AT&T's representations and promises, Mr. Terpin continued to maintain a wireless account with AT&T and to use his AT&T phone number for verification and other purposes.

181. As a direct and proximate result of AT&T's wrongful actions, Mr. Terpin has been damaged by paying monthly fees to AT&T and having thieves steal nearly $24 million worth of cryptocurrency through the January 7, 2018 SIM swap fraud.

182. AT&T's misconduct is fraud under Civil Code § 3294(c)(3) in that it was deceit or concealment of a material fact known to AT&T conducted with the intent on the part of AT&T of depriving Mr. Terpin of legal rights or otherwise causing injury. AT&T's conduct was done with malice, fraud or oppression under Civil Code § 3294(c)(1) and (2) and Mr. Terpin is entitled to punitive damages against AT&T under Civil Code §3294(a).

TENTH CLAIM FOR RELIEF

(Negligence)

183. Plaintiff realleges the allegations in Paragraphs 1 through 182 as if fully set forth herein.

184. AT&T owed a duty to Mr. Terpin to exercise reasonable care in safeguarding and protecting his Personal Information, including CPI and CPNI, and

keeping it from being compromised, lost, stolen, misused and/or disclosed to unauthorized parties. This duty included, among other things, designing, maintaining, and testing its security systems to ensure that Mr. Terpin's Personal Information, including CPI and CPNI, was adequately secured and protected. AT&T had a further duty to implement and adhere to the "high security" or "celebrity" protocol that it had promised Mr. Terpin that it would place on his account to protect his Personal Information and had a duty to adhere to the FCA, CPNI Rules, and the provisions of the Consent Decree.

185. AT&T knew that Mr. Terpin's Personal Information, including CPI and CPNI, was confidential and sensitive. Indeed, AT&T acknowledged this in its Privacy Policy and in agreeing, at Mr. Terpin's request, to place additional "high security" measures on Mr. Terpin's account to prevent hackers from committing SIM swap fraud on Mr. Terpin. AT&T further promoted its "extra security" on its website. AT&T likewise knew that Mr. Terpin's Personal Information was vulnerable to hacks by thieves and other criminals both because it acknowledged such in its Privacy Policy and because it had been informed by Mr. Terpin of the June 11, 2017 hack. AT&T thus knew of the substantial harms that could occur to Mr. Terpin if it did not place adequate security on his Personal Information and did not follow its own "high security" measures for the account.

186. By being entrusted by Mr. Terpin to safeguard his Personal Information, including CPI and CPNI, AT&T had a special relationship with Mr. Terpin. Mr. Terpin signed up for AT&T's wireless services and agreed to provide his Personal Information to AT&T with the understanding that AT&T would take appropriate measures to protect it. But AT&T did not protect Mr. Terpin's Personal Information and violated his trust. AT&T knew its security was inadequate in part due to the FCC investigation that led to the Consent Decree. AT&T is morally culpable, given prior security breaches involving its own employees.

GREENBERG GLUSKER FIELDS CLAMAN & MACHTINGER LLP
1900 Avenue of the Stars, 21st Floor
Los Angeles, California 90067-4590

187. AT&T breached its duty to exercise reasonable care in safeguarding and protecting Mr. Terpin's Personal Information, including CPI and CPNI, by failing to adopt, implement, and maintain adequate security measures to safeguard that information, including its duty under the FCA, CPNI Rules, the Consent Decree, and its own Privacy Policy.

188. AT&T's failure to comply with federal and state requirements for security further evidences AT&T's negligence in failing to exercise reasonable care in safeguarding and protecting Mr. Terpin's Personal Information, including CPI and CPNI.

189. But for AT&T's wrongful and negligent breach of its duties owed to Mr. Terpin, his Personal Information, including his CPI and CPNI, would not have been compromised, stolen, viewed, and used by unauthorized persons. AT&T's negligence was a direct and legal cause of the theft of Mr. Terpin's Personal Information and the legal cause of his resulting damages, including, but not limited to, the theft of nearly $24 million worth of cryptocurrency.

190. The injury and harm suffered by Mr. Terpin was the reasonably foreseeable result of AT&T's failure to exercise reasonable care in safeguarding and protecting Mr. Terpin's Personal Information, including his CPI and CPNI. The harm was additionally foreseeable in that AT&T was aware that Mr. Terpin was a holder and user of cryptocurrency and a potential victim of hacking following the June 11, 2017 hack.

191. AT&T's misconduct as alleged herein is malice, fraud or oppression under Civil Code § 3294(c)(1) and (2) in that it was despicable conduct carried on by AT&T with a willful and conscious disregard of the rights or safety of Mr. Terpin and despicable conduct that has subjected Mr. Terpin to cruel and unjust hardship in conscious disregard of his rights. As a result, Mr. Terpin is entitled to punitive damages against AT&T under Civil Code § 3294(a).

GREENBERG GLUSKER FIELDS CLAMAN & MACHTINGER LLP
1900 Avenue of the Stars, 21st Floor
Los Angeles, California 90067-4590

GREENBERG GLUSKER FIELDS CLAMAN
& MACHTINGER LLP
1900 Avenue of the Stars, 21st Floor
Los Angeles, California 90067-4590

ELEVENTH CLAIM FOR RELIEF

(Negligent Supervision and Training)

192. Mr. Terpin realleges the allegations of Paragraphs 1 through 191 as if fully set forth herein.

193. AT&T owed a duty to Mr. Terpin to exercise reasonable care in supervising and training its employees to safeguard and protect his Personal Information, including CPI and CPNI, and to keep it from being compromised, lost, stolen, misused and/or disclosed to unauthorized parties. This duty included AT&T's instructing its employees to adhere to the "high security" or "extra security" protocols that AT&T had promised Mr. Terpin it would place on his account to protect his Personal Information.

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

195. AT&T knew that Mr. Terpin's Personal Information, including CPI and CPNI, was confidential and sensitive. AT&T further knew that Mr. Terpin's Personal Information was vulnerable to hacks and SIM swap fraud by thieves and other criminals because it had been informed by Mr. Terpin of the June 11, 2017 hack.

196. By being entrusted by Mr. Terpin to safeguard his Personal Information, including CPI and CPNI, AT&T had a special relationship with Mr. Terpin. Mr. Terpin signed up for AT&T's wireless services and agreed to provide his Personal Information to AT&T with the understanding that AT&T's employees would take appropriate measures to protect it. AT&T also made promises in the COBC that its employees would respect its customers' privacy and was further required by the Consent Decree to supervise and train its employees to adhere to its legal obligations to protect their Personal Information.

GREENBERG GLUSKER FIELDS CLAMAN
& MACHTINGER LLP
1900 Avenue of the Stars, 21st Floor
Los Angeles, California 90067-4590

197. AT&T breached its duty to supervise and train its employees to safeguard and protect Mr. Terpin's Personal Information, including CPI and CPNI, by not requiring them to adhere to its obligations under the CPNI Rules, the Consent Decree and other legal provisions. On January 7, 2018, AT&T's employees facilitated SIM swap fraud on Mr. Terpin by not requiring individuals requesting Mr. Terpin's telephone number to present valid identification. AT&T employees also failed to follow AT&T's "higher" or "extra" security by not requiring the individual requesting Mr. Terpin's telephone number to provide the secret six-digit code that AT&T had given Mr. Terpin to prevent precisely such fraud.

198. AT&T knew its supervision and monitoring of its employees was inadequate through: a) the FCC investigation that led to the Consent Decree mandating measures to improve such training and monitoring; and b) its knowledge from prior incidents that its employees cooperated with hackers in SIM swap fraud. AT&T is morally culpable, given prior security breaches involving its own employees.

199. AT&T breached its duty to exercise reasonable care in supervising and monitoring its employees to protect Mr. Terpin's Personal Information, including CPI and CPNI.

200. AT&T's failure to comply with the Consent Decree and to follow the requirements of the FCA and CPNI Rules further evidence AT&T's negligence in adequately supervising and monitoring its employees so that they would safeguard and protect Mr. Terpin's Personal Information, including CPI and CPNI.

201. But for AT&T's wrongful and negligent breach of its duties to supervise and monitor its employees, Mr. Terpin's CPI and CPNI would not have been disclosed to unauthorized individuals through SIM swap fraud. AT&T's negligence was a direct and legal cause of the theft of Mr. Terpin's Personal

Information and the legal cause of his resulting damages, including, but not limited to, the theft of nearly $24 million worth of cryptocurrency.

202. The injury and harm suffered by Mr. Terpin was the reasonably foreseeable result of AT&T's failure to supervise and monitor its employees in safeguarding and protecting Mr. Terpin's Personal Information, including his CPI and CPNI.

203. AT&T's misconduct as alleged here is done with malice, fraud and oppression under Civil Code § 3294(c)(1) and (2) in that it was despicable conduct carried on by AT&T with a willful and conscious disregard of the rights or safety of Mr. Terpin and despicable conduct that has subjected Mr. Terpin to cruel and unjust hardship in conscious disregard of his rights. As a result, Mr. Terpin is entitled to punitive damages against AT&T under Civil Code § 3294(a).

TWELFTH CLAIM FOR RELIEF

(Negligent Hiring)

204. Mr. Terpin realleges the allegations in Paragraphs 1 through 203 as if fully set forth herein.

205. AT&T owed a duty to Mr. Terpin to exercise reasonable care in hiring competent, honest, and ethical employees to safeguard and protect his Personal Information, including CPI and CPNI, to keep it from being compromised, lost, stole, misused and/or disclosed to unauthorized parties. AT&T also owed a duty to exercise reasonable care in the operation of AT&T stores, including by third parties, and their hiring of employees for those AT&T stores.

206. AT&T knew that Mr. Terpin's Personal Information, including CPI and CPNI, was confidential and sensitive. AT&T further knew that Mr. Terpin's Personal Information was vulnerable to hacks and SIM swap fraud by thieves and other criminals because it had been informed by Mr. Terpin of the June 11, 2017 hack. AT&T further knew from the investigation that led to the Consent Decree that its employees had cooperated with hackers and thieves by turning over

GREENBERG GLUSKER FIELDS CLAMAN & MACHTINGER LLP
1900 Avenue of the Stars, 21st Floor
Los Angeles, California 90067-4590

to them the CPNI of its customers to facilitate fraud and theft. It also knew from prior incidents of SIM swap fraud that its employees cooperated with hackers and thieves defrauding AT&T's own customers.

207. By being entrusted by Mr. Terpin to safeguard his Personal Information, including CPI and CPNI, AT&T had a special relationship with Mr. Terpin. Mr. Terpin signed up for AT&T's wireless services and agreed to provide his Personal Information to AT&T with the understanding that AT&T's employees would take appropriate measures to protect it. AT&T also made promises in the COBC that its employees would adhere to AT&T's ethical and legal obligations, including respecting its customers' privacy. AT&T was further required by the Consent Decree to correct the practices that had led to hiring employees who had cooperated with hackers and thieves and stolen customers' personal information.

208. AT&T breached its duty to hire employees who would safeguard and protect Mr. Terpin's Personal Information, including CPI and CPNI. Mr. Terpin alleges on information and belief, that the employees who facilitated the SIM swap fraud perpetrated on Mr. Terpin did not live up to AT&T's purported ethical standards, as expressed in the COBC, or to their legal obligations to Mr. Terpin. Mr. Terpin further alleges on information and belief, that the employee at the AT&T store who ported Mr. Terpin's telephone number to the hackers on January 7, 2018, had a criminal record and colluded with the hackers in perpetrating the fraud on Mr. Terpin.

209. AT&T knew that its hiring of employees was inadequate through the FCC investigation that led to the Consent Decree that revealed that employees had actively handed over the Personal Information of its customers to hackers and thieves. AT&T is morally culpable, given the prior conduct of its employees.

GREENBERG GLUSKER FIELDS CLAMAN & MACHTINGER LLP
1900 Avenue of the Stars, 21st Floor
Los Angeles, California 90067-4590

210. AT&T breached its duty to properly hire competent, honest and ethical employees to protect Mr. Terpin's Personal Information, including CPI and CPNI.

211. AT&T's failure to comply with the Consent Decree is further evidence of its failure to investigate employees to ensure that they adhered to AT&T's ethical and legal responsibilities.

212. On information and belief, the employee at the AT&T store who gave Mr. Terpin's SIM card to the imposter on January 7, 2018 was Jahmil Smith. Smith has a criminal record which AT&T should have discovered before or after hiring him.

213. But for AT&T's wrongful and negligent breach of its duties to hire ethical and competent employees, Mr. Terpin's CPI and CPNI would not have been disclosed to unauthorized individuals through SIM swap fraud. AT&T's negligence was a direct and legal cause of the theft of Mr. Terpin's Personal Information and the legal cause of his resulting damages, including, but not limited to, the theft of nearly $24 million worth of cryptocurrency.

214. The injury and harm suffered by Mr. Terpin was the reasonably foreseeable result of AT&T's failure to hire competent and ethical employees who would safeguard and protect Mr. Terpin's Personal Information, including his CPI and CPNI. Indeed, this failure on the part of AT&T led to the January 7, 2018 SIM swap fraud.

215. AT&T's misconduct as alleged herein is malice, fraud and oppression under Civil Code § 3294(c)(1) and (2) in that it was despicable conduct carried on by AT&T with a willful and conscious disregard of the rights or safety of Mr. Terpin and despicable conduct that has subjected Mr. Terpin to cruel and unjust hardship in conscious disregard of his rights. As a result, Mr. Terpin is entitled to punitive damages against AT&T under Civil Code § 3294(a).

GREENBERG GLUSKER FIELDS CLAMAN & MACHTINGER LLP
1900 Avenue of the Stars, 21st Floor
Los Angeles, California 90067-4590

GREENBERG GLUSKER FIELDS CLAMAN
& MACHTINGER LLP
1900 Avenue of the Stars, 21st Floor
Los Angeles, California 90067-4590

THIRTEENTH CLAIM FOR RELIEF

(Breach of Contract – Privacy Policy)

216. Mr. Terpin realleges the allegations in Paragraphs 1 through 215 as if fully set forth herein.

217. The Privacy Policy is a binding contract between AT&T and Mr. Terpin.

218. AT&T breached the contract with respect to at least the following provisions of the Privacy Policy:

- AT&T's promise that it will not sell or disclose users' "Personal Information" to anyone;
- AT&T's commitments that it has "worked hard to protect your information" and has "established electronic and administrative safeguards designed to make the information we collect secure";
- AT&T's promise that its employees must follow its COBC and that "all employees must follow the laws, rules, regulations, court and/or administrative orders that apply to our business—including, specifically, the legal requirements and company policies surrounding the privacy of communications and the security and privacy of your records";
- AT&T's promise that it subjects employees who do not meet its security standards to "disciplinary action" and dismissal;
- AT&T's promise that it has "implemented technology and security features and strict policy guidelines to safeguard the privacy of your Personal Information";
- AT&Ts promise that it "maintain[s] and protect[s] the security of computer storage and network equipment";

- AT&T commitment that it limits access to Personal Information "to only those with jobs requiring such access"; and
- AT&T's promise that it "[r]equire[s] caller/online authentication before providing Account Information so that only you or someone who knows your Account Information will be able to access or change this information."

219. AT&T also breached its COBC by failing to follow "not only the letter of the law, but the spirit of the law" and failing to "protect the privacy of our customers' communications because "not only do our customers demand this, but the law requires it."

220. AT&T breached these provisions of its Privacy Policy and COBC by not having proper safeguards in accordance with law, including the FCA, CPNI Rules, and the Consent Decree, and Cal. Civ. Code §1798.81.5, to protect Mr. Terpin's "Personal Information," including CPI and CPNI. AT&T further breached its promises by not limiting access to Mr. Terpin's Personal Information to authorized or properly trained individuals. AT&T likewise violated its commitments to maintain the confidentiality and security of Mr. Terpin's Personal Information by failing to comply with its own policies and applicable "law, rules, regulations, court and/or administrative orders that apply to our business—including, specifically, the legal requirements and company policies surrounding the privacy of communications and the security and privacy of your records." AT&T thus breached its obligations under the FCA, CPNI Rules, the Consent Decree and California law.

221. The January 7, 2018 SIM swap fraud was a direct and legal cause of the injuries and damages suffered by Mr. Terpin, including loss of nearly $24 million of crypto currency.

GREENBERG GLUSKER FIELDS CLAMAN & MACHTINGER LLP
1900 Avenue of the Stars, 21st Floor
Los Angeles, California 90067-4590

GREENBERG GLUSKER FIELDS CLAMAN
& MACHTINGER LLP
1900 Avenue of the Stars, 21st Floor
Los Angeles, California 90067-4590

222. To the extent that AT&T maintains that the Exculpatory Provision, Damages Restriction, and the Indemnity in the Agreement apply to the promises made by AT&T in the Privacy Policy and the COBC, such provisions, as well as the Agreement in its entirety, are unenforceable and do not apply to the Privacy Policy and COBC. *See* Cal. Civ. Code §§1670.5, 1668 (contracts are unenforceable if unconscionable or void against public policy); *Ingle v. Circuit City Stores, Inc.*, 328 F.3d 1165, 1180 (9th Cir. 2003) (contracts void if central purpose is tainted with illegality). Moreover, such provisions are unconscionable under California law because an entity cannot exculpate itself from its obligations to maintain the privacy and security of personal information under federal and California law, as further set forth herein in Paragraphs 70 to 82. *See Health Net of California, Inc. v. Department of Health Services*, 113 Cal. App. 4th 224, 244 (2004) (California courts for 85 years have invalidated "contract clauses that relieve a party from responsibility for future statutory and regulatory violations")

223. Mr. Terpin was harmed due to AT&T's breach of the terms of the Privacy Policy and COBC, because his "Personal Information," including CPI and CPNI, was breached in the January 7, 2018 SIM swap fraud, which led to monetary losses of nearly $24 million.

FOURTEENTH CLAIM FOR RELIEF

(Breach of Implied Contracts

In the Alternative to Claim for Breach of Express Contract)

224. Mr. Terpin realleges the allegations of Paragraphs 1 through 223 as if fully set forth herein.

225. To the extent that AT&T's Privacy Policy and COBC did not form express contracts, the opening of an AT&T wireless account by Mr. Terpin created implied contracts between AT&T and Mr. Terpin as to the protection of his Personal Information, the terms of which were set forth by the relevant Privacy Policy and COBC.

GREENBERG GLUSKER FIELDS CLAMAN & MACHTINGER LLP
1900 Avenue of the Stars, 21st Floor
Los Angeles, California 90067-4590

226. AT&T breached such implied contracts by failing to adhere to the terms of the applicable Privacy Policy and COBC, as described above in Mr. Terpin's Thirteenth Claim for Relief. AT&T violated its commitment to maintain the confidentiality and security of the Personal Information of Mr. Terpin, including CPI and CPNI, and failed to comply with its own policies and "laws, rules, regulations, court and/or administrative orders that apply to [AT&T's] business—including, specifically, the privacy of communications and the security and privacy of your records." COBC.

227. Mr. Terpin was harmed because of AT&T's breach of the terms of the Privacy Policy and COBC, because his "Personal Information," including CPI and CPNI, were breached in the January 7, 2018 SIM swap fraud, which led to monetary losses of nearly $24 million.

FIFTEENTH CLAIM FOR RELIEF

(Breach of the Covenant of Good Faith and Fair Dealing)

228. Mr. Terpin realleges the allegations of Paragraphs 1 through 227 as if fully set forth herein.

229. Under California law, there is an implied covenant of good faith and fair dealing in every contract that neither party will do anything which will injure the right of the other to receive the benefits of the agreement.

230. Under the express and implied terms of the relationship between Mr. Terpin and AT&T, including through the Privacy Policy and COBC, Mr. Terpin and AT&T were to benefit using AT&T's services, while AT&T was supposed to benefit through money received for Mr. Terpin subscribing to AT&T's wireless services.

231. AT&T exhibited bad faith through its conscious awareness of and deliberate indifference to the risk to Mr. Terpin's Personal Information, including CPI and CPNI, by (a) not implementing security measures adequate to protect his Personal Information; (b) improperly hiring, training and supervising its

GREENBERG GLUSKER FIELDS CLAMAN & MACHTINGER LLP
1900 Avenue of the Stars, 21st Floor
Los Angeles, California 90067-4590

employees; (c) not adhering to its own security standards, including the "high security" standards for "high profile" or "celebrity" account holders; and (d) failing to invest in adequate security protections.

232. AT&T, by exposing Mr. Terpin to vastly greater security risks, breached its implied covenant of good faith and fair dealing with respect to the terms of its Privacy Policy and COBC and the implied warranties of their contractual relationship with their users.

233. Mr. Terpin was harmed because of AT&T's breach of the implied covenant of good faith and fair dealing because his Personal Information was compromised by the hackers in the January 7, 2018 SIM swap fraud which led to monetary damages of nearly $24 million.

234. AT&T's misconduct as alleged herein is fraud under Civil Code § 3294(c)(3) in that it was deceit or concealment of a material fact known to AT&T conducted with an intent on the part of AT&T of depriving Mr. Terpin of "legal rights or otherwise concerning injury." In addition, AT&T's misconduct, as alleged herein, is malice, fraud or oppression under Civil Code § 3294(c)(1) and (2) in that it was despicable conduct carried on by AT&T with a willful and conscious disregard of the rights or safety of Mr. Terpin and has subjected Mr. Terpin to cruel and unjust hardship in conscious disregard of his rights. As a result, Mr. Terpin is entitled to punitive damages against AT&T under Civil Code § 3294(a).

SIXTEENTH CLAIM FOR RELIEF

(Violation of California's Customer Records Act—Inadequate Security Cal. Civ. Code § 1798.81.5)

235. Mr. Terpin realleges the allegations of Paragraphs 1 through 234 as if fully set forth herein.

236. California Civil Code §1798.80 *et seq.*, known as the Customer Records Act ("CRA"), was enacted to "encourage businesses that own, license, or

maintain personal information about Californians to provide reasonable security for that information." Civil Code § 1798.81.5(a)(1).

237. Civil Code § 1798.81.5(b) requires any business that "owns, licenses or maintains personal information about a California resident" to "implement and maintain reasonable security procedures and practices appropriate to the nature of the information" and "to protect the personal information from unauthorized access, destruction, use, modification or disclosure." Civil Code § 1798.81.5(d)(1)(B) defines "personal information" as including account numbers, passwords and other sensitive information relating to individuals.

238. AT&T is a business that owns, licenses, or maintains the personal information of California residents. As alleged herein, AT&T did not "implement and maintain reasonable security procedures and practices" regarding Personal Information and protect it "from unauthorized access, destruction, use, modification or disclosure" as evidenced by the January 7, 2018 SIM swap fraud.

239. As a direct and legal result of AT&T's violation of Civil Code § 17981.81.5, Mr. Terpin was harmed because disclosure of his wireless account information allowed hackers to steal nearly $24 million worth of cryptocurrency.

240. Mr. Terpin seeks remedies available under Cal. Civ. Code § 1798.84, including, but not limited to damages suffered by him as alleged above and equitable relief.

241. AT&T's conduct is fraud under Civil Code § 3294(c)(3) in that it was deceit or concealment of a material fact known to AT&T conducted with the intent of AT&T to deprive Mr. Terpin of his legal rights or otherwise causing injury. Because the misconduct was done with malice, fraud and oppression, Mr. Terpin is entitled to punitive damages against AT&T under Civil Code § 3294(a).

GREENBERG GLUSKER FIELDS CLAMAN & MACHTINGER LLP
1900 Avenue of the Stars, 21st Floor
Los Angeles, California 90067-4590

GREENBERG GLUSKER FIELDS CLAMAN & MACHTINGER LLP
1900 Avenue of the Stars, 21st Floor
Los Angeles, California 90067-4590

PRAYER FOR RELIEF

Wherefore, Plaintiff Michael Terpin demands judgment against Defendants as follows:

1. For general damages against Defendants, and each of them, jointly and severally, in an amount to be determined at trial, but in no event less than $24,000,000;

2. For exemplary and punitive damages against Defendants, and each of them, in an amount to be determined at trial, but in no event greater than nine times the amount of general and special damages awarded to Plaintiff ($216 million);

3. For preliminary and permanent injunctive relief against Cross-Defendants, and each of them, enjoining and restraining them from continue to engage in unfair competition, unfair practices, violation of privacy, and other actions;

4. For a declaration that the Agreement in its entirety is unenforceable as unconscionable and against public policy or, in the alternative, that (a) the Exculpatory Provision is unenforceable as against Plaintiff; (b) the Damages Resolution is unenforceable against Plaintiff; and (c) the Indemnity is unenforceable against Mr. Terpin;

5. For attorney's fees under the FCA, California Penal Code § 202(e)(1), the California Legal Remedies Act and other applicable statutory provision;

6. For restitution, disgorgement of wrongfully obtained profits and injunctive relief pursuant to California Unfair Competition Law, Cal. Bus. & Prof. Code § 17200 *et seq.*;

7. For a declaration that AT&T's conduct violated the California Legal Remedies Act; and

8. For interest and costs of suit and such other and further relief as the Court deems just and proper.

DATED: August 15, 2018

GREENBERG GLUSKER FIELDS CLAMAN & MACHTINGER LLP

By:/s/Pierce O'Donnell
PIERCE O'DONNELL (SBN 081298)
Attorneys for Plaintiff Michael Terpin

GREENBERG GLUSKER FIELDS CLAMAN & MACHTINGER LLP
1900 Avenue of the Stars, 21st Floor
Los Angeles, California 90067-4590

DEMAND FOR JURY TRIAL

Plaintiff hereby requests a trial by jury.

DATED: August 15, 2018

GREENBERG GLUSKER FIELDS CLAMAN & MACHTINGER LLP

By:/s/ Pierce O'Donnell
PIERCE O'DONNELL (SBN 081298)
Attorneys for Plaintiff Michael Terpin

GREENBERG GLUSKER FIELDS CLAMAN & MACHTINGER LLP
1900 Avenue of the Stars, 21st Floor
Los Angeles, California 90067-4590