

1 PIERCE O'DONNELL (SBN 081298)  
 2 [PODonnell@GreenbergGlusker.com](mailto:PODonnell@GreenbergGlusker.com)  
 3 TIMOTHY J. TOOHEY (SBN 140117)  
 4 [TToohey@GreenbergGlusker.com](mailto:TToohey@GreenbergGlusker.com)  
 5 PAUL BLECHNER (SBN159514)  
 6 [PBlechner@GreenbergGlusker.com](mailto:PBlechner@GreenbergGlusker.com)  
 7 GREENBERG GLUSKER FIELDS CLAMAN &  
 8 MACHTINGER LLP  
 9 1900 Avenue of the Stars, 21st Floor  
 10 Los Angeles, California 90067-4590  
 11 Telephone: 310.553.3610  
 12 Fax: 310.553.0687

13 Attorneys for Plaintiff  
 14 **MICHAEL TERPIN**

15 UNITED STATES DISTRICT COURT  
 16 CENTRAL DISTRICT OF CALIFORNIA

17 GREENBERG GLUSKER FIELDS CLAMAN  
 18 & MACHTINGER LLP  
 19 1900 Avenue of the Stars, 21st Floor  
 20 Los Angeles, California 90067-4590

21 MICHAEL TERPIN,  
 22 Plaintiff,  
 23 v.  
 24 AT&T INC.; AT&T Mobility, LLC;  
 25 and DOES 1-25,  
 26 Defendants.

27 Case No. 2:18-cv-6975

28 **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,**

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

1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28

**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**

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

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

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

### 12 INTRODUCTION

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

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

27 5. More recently, AT&T employees are participating in a new  
28 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

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

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

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

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

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

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

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

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

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

26  
27  
28

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

1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28

**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.”

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

7           17. Over the past decade, AT&T has gone on a buying spree costing  
8 over \$150 billion, acquiring: Bell South (including Cingular Wireless and  
9 Yellowpages.com), Dobson Communications, Edge Wireless, Cellular One,  
10 Centennial, Wayport, Qualcomm Spectrum, Leap Wireless, DirecTV, and Iusacell  
11 and NII Holdings (now AT&T Mexico). During the same period, AT&T’s mobile  
12 phone business was rated as the worst among major providers. *Consumer Reports*  
13 named it the “worst carrier” in 2010, and the next year, J.D. Power found AT&T’s  
14 network the least reliable in the country—a dubious achievement that it also earned  
15 in prior years. Little wonder that its customers were the least happy of subscribers  
16 of the Big Four carriers according to the American Consumer Index. In the  
17 meantime, AT&T has purchased for a total equity value of \$85.4 billion Time  
18 Warner Inc.—the owner of HBO, Warner Bros, CNN, Turner Broadcasting,  
19 Cartoon Network, Turner Classic Movies, TBS, TNT and Turner Sports.

20           18. According to media reports, AT&T mobile telephone customers  
21 have been the subject of more privacy violations than subscribers to other cell  
22 phone companies. The Electronic Frontier Foundation has recently called out  
23 AT&T’s “hypocrisy” in calling for an “Internet Bill of Rights” when in fact “few  
24 companies have done more to combat privacy and network neutrality than AT&T.”  
25 <https://www.eff.org/deeplinks/2018/01/hypocrisy-atts-internet-bill-rights> AT&T  
26 has even lobbied the FCC to stop applying the privacy provisions of the FCA to its  
27 broadband services, while arguing (unsuccessfully) that it was not subject to the  
28 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

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

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

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

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

21 **FACTUAL ALLEGATIONS**

22 **AT&T’S STATUTORY OBLIGATION TO PROTECT**  
23 **CUSTOMERS’ PERSONAL INFORMATION**  
24 **UNDER THE FEDERAL COMMUNICATIONS ACT**

25 22. As a common carrier, AT&T is obligated to protect the  
26 confidential personal information of its customers under Section 222 of the FCA,  
27 47 U.S.C. § 222.  
28



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

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

15           25. Section 222(h)(1), 47 U.S.C. § 222(h)(1), defines CPNI as  
16 “(A) information that relates to the quantity, technical configuration, type,  
17 destination, location, and amount of use of a telecommunications service subscribed  
18 to by any customer of a telecommunications carrier, and that is made available to  
19 the carrier by the customer solely by virtue of the carrier-customer relationship; and  
20 (B) information contained in the bills pertaining to telephone exchange service or  
21 telephone toll service received by a customer of a carrier, except that term does not  
22 include subscriber list information.”

23           26. The FCC has promulgated rules to implement Section 222 “to  
24 ensure that telecommunications carriers establish effective safeguards to protect  
25 against unauthorized use or disclosure of CPNI.” *See* 47 CFR § 64.2001 *et seq.*  
26 (“CPNI Rules”); *CPNI Order*, 13 FCC Rcd. at 8195 ¶ 193. The CPNI Rules limit  
27 disclosure and use of CPNI without customer approval to certain limited  
28

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

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

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

21 29. The FCC has determined that information obtained from  
22 customers through a common social engineering ploy known as "pretexting" is  
23 CPNI. *See In the Matter of Implementation of the Telecommunications Acts of*  
24 *1996: Telecommunications Carriers' Use of Customer Proprietary Network*  
25 *Information and Other Customer Information*, 22 FCC Rcd. 6927 (2007)  
26 ("Pretexting Order"). Pretexting is "the practice of pretending to be a particular  
27 customer or other authorized person in order to obtain access to that customer's call  
28 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

1 “private communications” are CPI and CPNI under the FCA. *Id.* at 6928 *et seq.*  
2 The FCC concluded that “pretexters have been successful at gaining unauthorized  
3 access to CPNI” and that “carriers’ record on protecting CPNI demonstrate[d] that  
4 the Commission must take additional steps to protect customers from carriers that  
5 have failed to adequately protect CPNI.” *Id.* at 6933. The FCC modified its rules to  
6 impose additional security for carriers’ disclosure of CPNI and to require that law  
7 enforcement and customers be notified of security breaches involving CPNI. *Id.* at  
8 6936-62.

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

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

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

3 **AT&T EMPLOYEES’ DISCLOSURE OF CUSTOMERS’ PERSONAL**  
4 **INFORMATION AND THE APRIL 8, 2015 FCC CONSENT DECREE**

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

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

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

25 35. The FCC found that AT&T employees used their login  
26 credentials to access the confidential information of almost 280,000 customers.  
27 The FCC concluded that AT&T’s data security measures “failed to prevent or  
28 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

1           36. The FCC also found that AT&T had not properly supervised its  
2 employees’ access to its customers’ personal information, including CPNI. The  
3 FCC concluded that AT&T’s “failure to reasonably secure customers’ proprietary  
4 information violates a carrier’s statutory duty under the Communications Act to  
5 protect that information and constitutes an unjust and unreasonable practice in  
6 violation of the Act.” *Id.* at 2808 (Adopting Order § 2).

7           37. In the Adopting Order, the FCC emphasized the importance of  
8 AT&T’s obligation to adhere to the obligations embodied in Section 222 of the  
9 FCA. According to the Adopting Order, the purpose of Section 222 is to “ensure  
10 that consumers can trust that carriers have taken appropriate steps to ensure that  
11 unauthorized persons are not accessing, viewing or misusing their personal  
12 information.” *Id.* Carriers like AT&T are thus required to take “every reasonable  
13 precaution’ to protect their customers’ data” and to notify consumers regarding any  
14 breaches in order to “aid in the pursuit and apprehension of bad actors and provide  
15 valuable information that helps affected consumers [to] be proactive in protecting  
16 themselves in the aftermath of a data breach.” *Id.*

17           38. As a condition of terminating the FCC’s investigation of  
18 AT&T’s violations of Sections 201(b) and 222 of the FCA, the FCC imposed  
19 numerous requirements on AT&T to improve its supervision of employees and to  
20 adhere to its legal obligation to protect the privacy of AT&T’s customers.  
21 Moreover, the Consent Decree imposed obligations not only on AT&T itself, but  
22 also on AT&T’s “Covered Employees,” who are defined as “all employees and  
23 agents of AT&T who perform or directly supervise, oversee, or manage the  
24 performance of duties that involve access to, use, or disclosure of Personal  
25 Information or Customer Proprietary Network Information at Call Centers managed  
26 and operated by AT&T Mobility.” *Id.* at 2811. “Call Center” is defined broadly in  
27 the Consent Decree as call centers operated by AT&T or its contractors “that  
28

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

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

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

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

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

- 18 (i) administrative, technical, and physical safeguards reasonably  
19 designed to protect the security and confidentiality of Personal  
20 Information and CPNI;  
21 (ii) reasonable measures to protect Personal Information and CPNI  
22 maintained by or made available to Vendors, Covered Employees, and  
23 Covered Vendor Employees. . . ;  
24 (iii) access controls reasonably designed to limit access to Personal  
25 Information and CPNI to authorized AT&T employees, agents, and  
26 Covered Vendor Employees;  
27 (iv) reasonable processes to assist AT&T in detecting and responding  
28 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

1 malware or otherwise, involving Covered Employees and Covered  
2 Vendor Employees; and  
3 (v) a comprehensive breach response plan that will enable AT&T to  
4 fulfill its obligations under applicable laws, with regard to breach  
5 notifications, including its obligations under paragraph 20 while that  
6 paragraph remains in effect.

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

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

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

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

14 **AT&T’S PRIVACY AND SECURITY COMMITMENTS TO CUSTOMERS**  
 15 **IN ITS PRIVACY POLICY AND CODE OF BUSINESS CONDUCT**

16 45. In its Privacy Policy (“Privacy Policy”) and Code of Business  
 17 Conduct (“COBC”), AT&T acknowledges its responsibilities to protect customers’  
 18 “Personal Information” under the FCA, the CPNI Rules and other regulations. A  
 19 true and correct copy of the Privacy Policy in effect in January 2018 available at  
 20 [http://about.att.com/sites/privacy\\_policy](http://about.att.com/sites/privacy_policy) is attached hereto as Exhibit B. A true  
 21 and correct copy of the COBC in effect in January 2018 available at  
 22 <https://ebiznet.sbc.com/attcode/index.cfm> is attached hereto as Exhibit C.

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



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

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

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

14 We’ve worked hard to protect your information. *And we’ve established*  
15 *electronic and administrative safeguards designed to make the information*  
16 *we collect secure.* Some examples of those safeguards include:

- 17 • All of our employees are subject to the AT&T Code of Business  
18 Conduct (COBC)

19 ([https://www.att.com/Common/about\\_us/downloads/att\\_code\\_of\\_busi](https://www.att.com/Common/about_us/downloads/att_code_of_business_conduct.pdf)  
20 [ness\\_conduct.pdf](https://www.att.com/Common/about_us/downloads/att_code_of_business_conduct.pdf)) and certain state-mandated codes of conduct.

21 Under the COBC, all employees must follow the laws, rules,  
22 regulations, court and/or administrative orders that apply to our  
23 business—including, specifically, the legal requirements and company  
24 policies surrounding the privacy of communications and the security  
25 and privacy of your records. We take this seriously, and any of our  
26 employees who fail to meet the standards we’ve set in the COBC are  
27 subject to disciplinary action. That includes dismissal.  
28

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

1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28

• 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.*

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

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

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

### 18 **THE PREVALENCE OF SIM CARD SWAP FRAUD**

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

25 53. As described in in a July 30, 2018 article in *Motherboard*  
 26 entitled “‘Tell Your Dad to Give Us Bitcoin:’ How a Hacker Allegedly Stole  
 27 Millions by Hijacking Phone Numbers,” available at  
 28 [https://motherboard.vice.com/en\\_us/article/a3q7mz/hacker-allegedly-stole-](https://motherboard.vice.com/en_us/article/a3q7mz/hacker-allegedly-stole-)

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

9           54. The leading security reporter Brian Krebs wrote on August 18,  
10 2018 ([https://krebsonsecurity.com/2018/08/florida-man-arrested-in-sim-swap-  
11 conspiracy/](https://krebsonsecurity.com/2018/08/florida-man-arrested-in-sim-swap-conspiracy/)) that “SIM swaps are frequently abused by scam artists who trick  
12 mobile providers into tying a target’s service to a new SIM card and mobile phone  
13 that the attackers control. Unauthorized SIM swaps often are perpetrated by  
14 fraudsters who have already stolen or phished a target’s password, as many banks  
15 and online services rely on text messages to send users a one-time code that needs  
16 to be entered in addition to a password for online authentication.” As Mr. Krebs  
17 also wrote: “[i]n some cases, fraudulent SIM swaps succeed thanks to lax  
18 authentication procedures at mobile phone stores. *In other instances, mobile store  
19 employees work directly with cyber criminals to help conduct unauthorized SIM  
20 swaps. . . .*” (Emphasis added.)

21           55. Mr. Terpin alleges on information and belief that AT&T knew  
22 well before the attacks on Mr. Terpin that it was subject to widespread SIM swap  
23 fraud. Mr. Terpin alleges further that AT&T knew that cryptocurrency investors  
24 like Plaintiff were specifically targeted by SIM swapping and that AT&T was the  
25 weak link in such fraud. This is confirmed in numerous articles on SIM swap  
26 fraud, including that of Brian Krebs and a July 31, 2018 article in bitcoinist.com  
27 entitled “Sim-Swapping Bitcoin Thief Charged in California Court,” available at  
28 <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

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

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

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

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

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

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

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

24 61. Mr. Terpin alleges on information and belief that AT&T is fully  
25 aware of these and numerous other SIM swapping incidents involving its  
26 customers, including incidents where its own employees were complicit with  
27 hackers. For example, the *Motherboard* article confirms that AT&T had provided  
28 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

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

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

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

14 **THE JUNE 11, 2017 HACK**

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

22 65. After the hackers took charge of Mr. Terpin’s telephone number,  
23 the hackers accessed Mr. Terpin’s telephone to divert texts and telephone calls to  
24 gain access to Mr. Terpin’s cryptocurrency accounts. The hackers also used the  
25 phone to hijack Mr. Terpin’s Skype account to impersonate him. By that means,  
26 the hackers convinced a client of Mr. Terpin to send them cryptocurrency and  
27 diverted a payment due to Mr. Terpin to themselves. AT&T finally cut off access  
28

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

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

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

25 68. As alleged above, AT&T was well aware at the time of the June  
26 11, 2017 incident that its users were subject to SIM swap fraud. It was also well  
27 aware that its employees cooperated in such fraud and that the employees could  
28 bypass its security procedures. Mr. Terpin alleges on information and belief that



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

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

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

#### 26 **THE JANUARY 7, 2018 SIM SWAP FRAUD**

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

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

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

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

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

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

26           76. Because of AT&T's cooperation and failure to follow its own  
27 policies, the hackers were able to intercept Mr. Terpin's personal information,  
28

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

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

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

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

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

21 **FIRST CLAIM FOR RELIEF**

22 **(Declaratory Relief:**

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

25 80. Mr. Terpin brings this claim for declaratory relief under 28  
26 U.S.C. § 2201 to have the Court declare that AT&T’s wireless customer agreement  
27 (the “Agreement”) is unconscionable, void against public policy under Cal. Civ.  
28 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

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

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

11           83. The version of the Agreement posted in early 2018 purports to  
12 govern AT&T's provision of wireless service to all customers, including Mr.  
13 Terpin who first contracted with AT&T over two decades ago. A true and correct  
14 copy of the Agreement posted on AT&T's website in early 2018 at  
15 <https://www.att.com/legal/terms.wirelessCustomerAgreement-list.html> is attached  
16 hereto as Exhibit D. As alleged below, the Agreement contains numerous  
17 unconscionable terms that renders it unenforceable in its entirety because its  
18 "central purpose . . . is tainted with illegality." *Ingle v. Circuit City Stores, Inc.*,  
19 328 F.3d 1165, 1180 (9<sup>th</sup> Cir. 2003) (holding invalid an agreement that obstructs the  
20 ability of customers to bring any claims against defendant).

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

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

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

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

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

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

22 ***WE DO NOT GUARANTEE YOU UNINTERRUPTED SERVICE***  
23 ***OR COVERAGE. . . . AT&T MAKES NO WARRANTY,***  
24 ***EXPRESS OR IMPLIED, OF MERCHANTABILITY OR FITNESS***  
25 ***FOR A PARTICULAR PURPOSE, SUITABILITY, ACCURACY,***  
26 ***SECURITY OR PERFORMANCE REGARDING ANY SERVICES,***  
27 ***SOFTWARE OR GOODS, AND IN NO EVENT SHALL AT&T BE***  
28

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

- 1                   ***LIABLE, WHETHER OR NOT DUE TO ITS OWN NEGLIGENCE,***
- 2                   for any:
- 3                   a. act or omission of a third party;
- 4                   b. mistakes, omissions, interruptions, errors, failures to transmit,
- 5                   delays, or defects in the Services or Software provided by or through
- 6                   us;
- 7                   c. ***damages or injury caused by the use of Services, Software, or***
- 8                   ***Device***, including use in a vehicle . . .

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

10                   88. The Exculpatory Provision renders the entire Agreement

11 unenforceable on public policy grounds under Cal. Civil Code §§ 1668 and 1670.5

12 because it purports to exempt AT&T from its gross negligence, statutory violations

13 and willful behavior, including the egregious conduct alleged herein. The

14 Exculpatory Provision is further against public policy because it purports to exempt

15 AT&T from violation of statutory obligations, including the obligation to maintain

16 the confidentiality and security of its customers’ private and personal information

17 under Section 222 of the FCA, the FCC Consent Degree, and numerous provisions

18 of California State law, including California unfair competition law, the Consumer

19 Legal Remedies Act, and the California Customer Records Act. Thus, even where,

20 as here, AT&T willfully violates its statutory duties under the FCA and the Consent

21 Decree, not to mention its promises in its Privacy Policy and the COBC, a customer

22 is prevented by the Exculpatory Provision from bringing a claim for negligent or

23 willful disclosure of the customer’s Personal Information, including CPNI, because

24 such claim seeks redress for “damages or injury caused by the use of Services,

25 Software, or Device . . .” and is waived by the Exculpatory Provision.

26                   89. AT&T also seeks in the contract to have customers waive any

27 damages, except for providing a “credit equal to a pro-rata adjustment of the

28

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

1 monthly Services fee for the time period your Services was unavailable, not to  
2 exceed the monthly Service fee” when a customer’s services are interrupted.

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

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

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

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



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

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

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

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

28 (Capitalization in original; emphasis added.)

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

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

12           96. Because the entire Agreement is unenforceable because the  
13 central purpose of the Agreement is “tainted with illegality . . . [so that] the contract  
14 as a whole cannot be enforced,” the arbitration provision in Paragraph 2.2 of the  
15 Agreement (“Arbitration Provision”) is also enforceable. *See, Armendariz*, 24 Cal.  
16 4<sup>th</sup> at 89-90.

17           97. The Arbitration Provision would require Mr. Terpin to arbitrate  
18 his claims “without affording the full range of statutory remedies, including  
19 punitive damages and attorney fees” that are available to him under the claims  
20 alleged herein. *Armendariz*, 24 Cal. 4<sup>th</sup> at 103 (damages limitation unlawful if  
21 applied to statutory claims). For example, Mr. Terpin, if required to arbitrate this  
22 claim, would be forced by the Damages Limitation to forego his statutory  
23 entitlement to punitive damages under his Third Claim for Relief under California  
24 Penal Code § 502 *et seq.* and to his entitlement to punitive damages for AT&T’s  
25 fraud and negligence. Moreover, the Arbitration Provision would require Mr.  
26 Terpin to forego the full range of damages to which he is entitled under his Second  
27 Claim for Relief under the Federal Communications Act § 222. These defects  
28

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

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

3 98. Because the defenses raised by Mr. Terpin as to the  
4 unconscionability of the Agreement are “enforced evenhandedly” and do not  
5 “interfere[] with the fundamental attributes of arbitration,” they do not run afoul of  
6 *AT&T Mobility LLC v. Concepcion*, 563 U.S. 333 (2010). The Court’s decision in  
7 *Concepcion* did not abrogate the savings clause of the FAA that provides that  
8 arbitration agreements may be declared unenforceable “upon such grounds as exist  
9 at law or in equity for the revocation of any contract,” including “generally  
10 applicable contract defenses, such as fraud, duress, or unconscionability.”  
11 *Concepcion* at 339, quoting 9 U.S.C. § 2 and *Doctors Associates, Inc. v. Casarotto*,  
12 517 U.S. 681, 687 (1996). For the reasons alleged in this claim, such defenses  
13 apply squarely to the Agreement.

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

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

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

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

3 **SECOND CLAIM FOR RELIEF**

4 **(Unauthorized Disclosure of Customer Confidential Proprietary Information**  
5 **and Proprietary Network Information**  
6 **(Federal Communications Act, 47 U.S.C. §§ 206, 222))**

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

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

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

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

24 106. Section 222(c)(1) of the FCA, 47 U.S.C. § 222(c)(1) further  
25 requires that, “[e]xcept as required by law or with the approval of the customer, a  
26 telecommunications carrier that receives or obtains customer proprietary  
27 information by virtue of its provision of a telecommunications service shall only  
28 use, disclose, or permit access to customer proprietary network information

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

4 107. The information disclosed to hackers by AT&T in the January 7,  
5 2018 SIM swap fraud transferring Mr. Terpin’s telephone number, was CPI and  
6 CPNI under Section 222 of the FCA.

7 108. AT&T failed to protect the confidentiality of Mr. Terpin’s CPI  
8 and CPNI, including his wireless telephone number, account information, and his  
9 private communications, by divulging that information to hackers in the January 7,  
10 2018 SIM swap fraud. Through its negligence, gross negligence and deliberate  
11 acts, including inexplicable failures to follow its own security procedures, supervise  
12 its employees, the CPNI Regulations, the terms of the Consent Decree, the  
13 warnings of the Pretexting Order, its Privacy Policy and the COBC, and by  
14 allowing its employees to bypass such procedures, AT&T permitted hackers to  
15 access Mr. Terpin’s telephone number, telephone calls, text messages and account  
16 information to steal nearly \$24,000,000 worth of his cryptocurrency.

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

21 110. Mr. Terpin is also entitled to his attorney’s fees under the FCA  
22 in bringing this action against AT&T for its gross negligence and fraudulent  
23 misrepresentation as to the security that it provides for customer accounts as  
24 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

25  
26  
27  
28

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

1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28

**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

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

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

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

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

25 119. What is truly mystifying here is how the hacker for the January  
26 7, 2018 crime could get Mr. Terpin's telephone number on the first try. Back on  
27 July 11, 2017, the criminals were unable to get the number even though they visited  
28 *11 stores*. Most likely, as AT&T knew, the January 7, 2018 hacker was an inside

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

3 120. Because of the conduct alleged herein by AT&T, Mr. Terpin is  
4 entitled to compensatory damages and injunctive relief under Penal Code §  
5 502(e)(1). Mr. Terpin is also entitled to reasonable attorney fees pursuant to Penal  
6 Code § 502(e)(2).

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

11 **FOURTH CLAIM FOR RELIEF**  
12 **(Violation of California Unfair Competition Law**  
13 **Unlawful Business Practice**  
14 **Cal. Bus. & Prof. Code § 17200 *et seq.*)**

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

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

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

26 125. AT&T falsely represented to Mr. Terpin and other customers in  
27 its Privacy Policy and COBC: (a) that its system was secure and that it would  
28 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



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

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

18           127. AT&T misrepresented to Mr. Terpin after the June 11, 2017  
19 incident that it had added “special protection” to protect Mr. Terpin’s “celebrity” or  
20 “high profile” account. These increased security measures included requiring a six-  
21 digit passcode to ensure that Mr. Terpin’s account would not readily be hacked,  
22 including by someone spoofing his identity and attempting to transfer his telephone  
23 number to their phone. In fact, AT&T’s representations were false because an  
24 imposter was readily able to obtain Mr. Terpin’s wireless number from a  
25 cooperative (or wantonly incompetent) employee at an AT&T facility on January 7,  
26 2018 without having either proper identification or being asked to provide the  
27 required six-digit passcode.  
28

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

1           128. Even without AT&T’s misrepresentations after the June 11,  
2 2017 hack, Mr. Terpin was entitled to assume that AT&T would take appropriate  
3 measures to keep secure his Personal Information, including CPI and CPNI,  
4 because of its statements in its Privacy Policy and COBC. AT&T did not disclose  
5 at any time that Mr. Terpin’s CPI and CPNI were vulnerable to hackers because  
6 AT&T’s security measures were ineffective. AT&T, which was the only party in  
7 possession of material information as to its own practices, did not disclose the  
8 rampant defects in its security procedures, including the ability of its employees to  
9 bypass such procedures, when it had a duty to do so. AT&T further violated the  
10 UCL by failing to implement reasonable and appropriate security measures for Mr.  
11 Terpin’s Personal Information, as required by the FCA, the CPNI Rules, the  
12 Consent Decree and California law, or following industry standards for data  
13 security, and failing to comply with its own Privacy Policy and COBC. If AT&T  
14 had complied with these legal requirements, Mr. Terpin would not have suffered  
15 the damages related to the January 7, 2018 SIM swap fraud.

16           129. AT&T’s acts, omissions, and misrepresentations as alleged  
17 herein were unlawful and in violation of, *inter alia*, the FCA, 47 U.S.C. §§ 206 and  
18 222, the CPNI Rules, the Consent Decree, Cal. Civ. Code § 1798.81.5(b), Section  
19 5(a) of the Federal Trade Commission Act, 15 U.S.C. § 45(a), Cal. Bus. & Prof.  
20 Code § 22576 (because of AT&T failing to comply with its own posted privacy  
21 policies), and the Consumer Legal Remedies Act, Cal. Civ. Code § 1750 *et seq.*

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

27  
28

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

4 **FIFTH CLAIM FOR RELIEF**

5 **(Violation of California Unfair Competition Law**

6 **Unfair Business Practice**

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

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

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

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

26 135. AT&T further assured Mr. Terpin, after the June 11, 2017 hack,  
27 that his Personal Information, including CPI and CPNI, was secure because AT&T  
28

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

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

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

13 137. AT&T knew or should have known that it did not employ  
14 reasonable security and lacked adequate employee training and monitoring  
15 measures that would have kept Mr. Terpin’s personal and financial information  
16 secure and prevented the loss or misuse of Mr. Terpin’s Personal information.  
17 AT&T had been put on notice through the Consent Decree and by the June 11,  
18 2017 hack of its lax security practices and inadequate training and supervision of  
19 employees. AT&T’s system is less secure than the access portals for numerous  
20 gyms, which require fingerprint identification for entrance.

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

1 swap fraud. Moreover, if AT&T had followed the higher security measures it  
2 purportedly employed after the June 11, 2017 hack, Mr. Terpin would not have  
3 suffered the damages from the January 7, 2018 SIM swap fraud.

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

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

13 141. AT&T's actions and omissions, as described above, violated  
14 fundamental public policies expressed by the United States and California. *See,*  
15 *e.g.*, FCA, 47 U.S.C. § 222; CPNI Rules; Consent Decree; Cal. Civ. Code § 1798.1  
16 ("The [California] Legislature declares that . . . all individuals have a right of  
17 privacy in information pertaining to them . . . The increasing use of computers . . .  
18 has greatly magnified the potential risk to individual privacy that can occur from  
19 the maintenance of personal information); Cal. Civ. Code § 1798.81.5(a) ("It is the  
20 intent of the Legislature to ensure that personal information about California  
21 residents is protected."); Cal. Bus. & Prof. Code § 22578 ("It is the intent of the  
22 Legislature that this chapter [including the Online Privacy Protection Act] is a  
23 matter of statewide concern.) Defendants' acts and omission, and the injuries  
24 caused by them, are thus "comparable to or the same as a violation of law. . ." *Cel-*  
25 *Tech Communications, Inc. v. Los Angeles Cellular Telephone Co.*, 20 Cal. 4<sup>th</sup> 163,  
26 187 (1999).

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

1 nearly \$24 million in actual financial harm because of AT&T’s unfair business  
2 practices.

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

6 **SIXTH CLAIM FOR RELIEF**

7 **(Violation of California Unfair Competition Law**

8 **Fraudulent Business Practice**

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

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

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

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

27 147. AT&T’s misrepresentations and fraudulent conduct were  
28 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

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

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

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

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

23 151. Mr. Terpin relied upon the representations that AT&T made  
24 after the June 11, 2017 hack and in the Privacy Policy and COBC. Based on the  
25 representations that AT&T was implementing a higher level of security, Mr. Terpin  
26 was entitled to, and did, assume AT&T would take appropriate measures to keep  
27 his Personal Information safe, including not handing over his wireless number that  
28 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

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

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

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

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

16 **SEVENTH CLAIM FOR RELIEF**

17 **(Violation of California Consumer Legal Remedies Act (“CLRA”))**

18 **Cal. Civ. Code § 1750 *et seq.*)**

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

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

26 157. Mr. Terpin is a consumer within the meaning of Cal. Civ. Code  
27 § 1761(d).

28



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

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

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

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

26           161. AT&T knew or should have known that it did not employ  
27 reasonable measures to keep Mr. Terpin’s Personal Information secure and prevent  
28 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

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

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

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

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

**EIGHTH CLAIM FOR RELIEF**

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

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

22 166. As alleged above, AT&T knew that its data security measures  
23 were grossly inadequate, that its employees could readily bypass the procedures,  
24 that its employees actively cooperated with hackers and thieves, and that it was  
25 incapable of living up to its commitments to consumers, including to Mr. Terpin,  
26 under state and federal law, as well as under its own Privacy Policy, to protect his  
27 Personal Information, including CPI and CPNI.  
28

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

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

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

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

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

19 171. Had AT&T disclosed the true facts about its dangerously poor  
20 data security practices and its inadequate supervision and training of its employees,  
21 Mr. Terpin would have taken further measures to protect himself. Mr. Terpin  
22 justifiably relied on AT&T’s statements, including statements after the June 11,  
23 2017 hack, and further relied on AT&T to provide accurate and complete  
24 information about its data security.

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

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

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

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

3 174. Because of the deceit by AT&T, it is liable under Cal. Civ. Code  
4 § 1709 for “any damage which [Mr. Terpin] thereby suffers.”

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

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

16 **NINTH CLAIM FOR RELIEF**

17 **(Misrepresentation)**

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

20 178. As outlined above, AT&T made numerous representations and  
21 false promises in its Privacy Policies and COBC as well as in its advertising,  
22 regarding the supposed security of consumers’ Personal Information, including Mr.  
23 Terpin’s Personal Information, and when an AT&T employee persuaded Mr.  
24 Terpin not to cancel his service after the June 11, 2017 hack. Such representations  
25 and promises were false because AT&T was using outdated security procedures and  
26 failed to disclose that it did not adhere to its own standards, including the  
27 heightened security standards that it implemented for Mr. Terpin after the June 11,  
28 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

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

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

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

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

23 **TENTH CLAIM FOR RELIEF**

24 **(Negligence)**

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

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

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

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

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

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

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

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

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

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

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

22 191. AT&T’s misconduct as alleged herein is malice, fraud or  
23 oppression under Civil Code § 3294(c)(1) and (2) in that it was despicable conduct  
24 carried on by AT&T with a willful and conscious disregard of the rights or safety of  
25 Mr. Terpin and despicable conduct that has subjected Mr. Terpin to cruel and unjust  
26 hardship in conscious disregard of his rights. As a result, Mr. Terpin is entitled to  
27 punitive damages against AT&T under Civil Code § 3294(a).  
28

**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

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

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

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

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

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

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

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

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

### 13 TWELFTH CLAIM FOR RELIEF

#### 14 (Negligent Hiring)

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

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

23 206. AT&T knew that Mr. Terpin's Personal Information, including  
24 CPI and CPNI, was confidential and sensitive. AT&T further knew that Mr.  
25 Terpin's Personal Information was vulnerable to hacks and SIM swap fraud by  
26 thieves and other criminals because it had been informed by Mr. Terpin of the June  
27 11, 2017 hack. AT&T further knew from the investigation that led to the Consent  
28 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

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

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

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

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

27  
28

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

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

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

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

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

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

22           215. AT&T’s misconduct as alleged herein is malice, fraud and  
23 oppression under Civil Code § 3294(c)(1) and (2) in that it was despicable conduct  
24 carried on by AT&T with a willful and conscious disregard of the rights or safety of  
25 Mr. Terpin and despicable conduct that has subjected Mr. Terpin to cruel and unjust  
26 hardship in conscious disregard of his rights. As a result, Mr. Terpin is entitled to  
27 punitive damages against AT&T under Civil Code § 3294(a).  
28

**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&T’s promise that it “maintain[s] and protect[s] the security of computer storage and network equipment”;

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

- 1                   • AT&T commitment that it limits access to Personal
- 2                   Information “to only those with jobs requiring such access”;
- 3                   and
- 4                   • AT&T’s promise that it “[r]equire[s] caller/online
- 5                   authentication before providing Account Information so that
- 6                   only you or someone who knows your Account Information
- 7                   will be able to access or change this information.”

8                   219. AT&T also breached its COBC by failing to follow “not only

9                   the letter of the law, but the spirit of the law” and failing to “protect the privacy of

10                  our customers’ communications because “not only do our customers demand this,

11                  but the law requires it.”

12                  220. AT&T breached these provisions of its Privacy Policy and

13                  COBC by not having proper safeguards in accordance with law, including the FCA,

14                  CPNI Rules, and the Consent Decree, and Cal. Civ. Code §1798.81.5, to protect

15                  Mr. Terpin’s “Personal Information,” including CPI and CPNI. AT&T further

16                  breached its promises by not limiting access to Mr. Terpin’s Personal Information

17                  to authorized or properly trained individuals. AT&T likewise violated its

18                  commitments to maintain the confidentiality and security of Mr. Terpin’s Personal

19                  Information by failing to comply with its own policies and applicable “law, rules,

20                  regulations, court and/or administrative orders that apply to our business—

21                  including, specifically, the legal requirements and company policies surrounding

22                  the privacy of communications and the security and privacy of your records.”

23                  AT&T thus breached its obligations under the FCA, CPNI Rules, the Consent

24                  Decree and California law.

25                  221. The January 7, 2018 SIM swap fraud was a direct and legal

26                  cause of the injuries and damages suffered by Mr. Terpin, including loss of nearly

27                  \$24 million of crypto currency.

28







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

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

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

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

12 234. AT&T’s misconduct as alleged herein is fraud under Civil Code  
13 § 3294(c)(3) in that it was deceit or concealment of a material fact known to AT&T  
14 conducted with an intent on the part of AT&T of depriving Mr. Terpin of “legal  
15 rights or otherwise concerning injury.” In addition, AT&T’s misconduct, as alleged  
16 herein, is malice, fraud or oppression under Civil Code § 3294(c)(1) and (2) in that  
17 it was despicable conduct carried on by AT&T with a willful and conscious  
18 disregard of the rights or safety of Mr. Terpin and has subjected Mr. Terpin to cruel  
19 and unjust hardship in conscious disregard of his rights. As a result, Mr. Terpin is  
20 entitled to punitive damages against AT&T under Civil Code § 3294(a).

21 **SIXTEENTH CLAIM FOR RELIEF**

22 **(Violation of California’s Customer Records Act—Inadequate Security**

23 **Cal. Civ. Code § 1798.81.5)**

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

26 236. California Civil Code §1798.80 *et seq.*, known as the Customer  
27 Records Act (“CRA”), was enacted to “encourage businesses that own, license, or  
28

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

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

3 237. Civil Code § 1798.81.5(b) requires any business that “owns,  
4 licenses or maintains personal information about a California resident” to  
5 “implement and maintain reasonable security procedures and practices appropriate  
6 to the nature of the information” and “to protect the personal information from  
7 unauthorized access, destruction, use, modification or disclosure.” Civil Code §  
8 1798.81.5(d)(1)(B) defines “personal information” as including account numbers,  
9 passwords and other sensitive information relating to individuals.

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

15 239. As a direct and legal result of AT&T’s violation of Civil Code §  
16 1798.81.5, Mr. Terpin was harmed because disclosure of his wireless account  
17 information allowed hackers to steal nearly \$24 million worth of cryptocurrency.

18 240. Mr. Terpin seeks remedies available under Cal. Civ. Code §  
19 1798.84, including, but not limited to damages suffered by him as alleged above  
20 and equitable relief.

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

26  
27  
28

1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28

**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

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

1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28

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

1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28

**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