

1 PIERCE O'DONNELL (SBN 081298)  
 2 PODonnell@GreenbergGlusker.com  
 3 TIMOTHY J. TOOHEY (SBN 140117)  
 4 TToohey@GreenbergGlusker.com  
 5 PAUL BLECHNER (SBN159514)  
 6 PBlechner@GreenbergGlusker.com  
 7 GREENBERG GLUSKER FIELDS CLAMAN &  
 8 MACHTINGER LLP  
 9 2049 Century Park East, Suite 2600  
 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 WESTERN DIVISION

18 MICHAEL TERPIN,  
 19 Plaintiff,  
 20 v.  
 21 AT&T MOBILITY, LLC; and DOES  
 22 1-25,  
 23 Defendants.

Case No. 2:18-cv-06975-ODW-KS

**PLAINTIFF'S OPPOSITION TO  
 MOTION TO DISMISS THE  
 SECOND AMENDED COMPLAINT  
 OF DEFENDANT AT&T  
 MOBILITY, LLC.**

[Fed. R. Civ. Proc. 12(b)(6)]

*Assigned To:*  
 Honorable Otis D. Wright II

Hearing: May 4, 2020  
 Time: 1:30 p.m.  
 Dept./Place: 350 West 1<sup>st</sup> Street  
 5<sup>th</sup> Floor, Courtroom 5D  
 Los Angeles, CA 90012

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

24  
25  
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

## TABLE OF CONTENTS

- I. INTRODUCTION ..... 1
- II. ARGUMENT ..... 2
  - A. Mr. Terpin Has Appropriately Alleged Deceit by Concealment. .... 2
    - 1. Mr. Terpin alleges that AT&T deceived him after the June 11, 2017 hack. .... 2
    - 2. AT&T Had a Duty to Disclose Material Facts. .... 5
    - 3. Mr. Terpin Has Adequately Plead that he was Unaware of Concealed Material Facts. .... 9
  - B. Mr. Terpin Has Adequately Plead His Fourth Claim for Relief for Misrepresentation. .... 10
    - 1. Mr. Terpin Adequately Alleges Reliance. .... 10
    - 2. Mr. Terpin has Adequately Alleged that AT&T’s statements were known to be false. .... 11
  - C. Mr. Terpin Has Properly Alleged Punitive Damages. .... 13
    - 1. Mr. Terpin’s Alleges Punitive Damages Based on the Actions of AT&T’s Officers and Managing Agents. .... 13
      - a. AT&T Has Violated Its Obligations Under Law By Allowing Its Employees to Turn Over its Customers’ Personal Information. .... 14
      - b. AT&T’s Corporate Officers Deliberately Perpetuated A Grossly Inadequate Security System. .... 15
      - c. The SAC Adequately Alleges that Employees Can Readily Evade or Bypass AT&T’s Security System. .... 16
    - 2. Cases Involving the Ratification of the Actions of Low-Level Employees are Not Relevant. .... 17
    - 3. Mr. Terpin Has Adequately Alleged Malice, Oppression and Fraud by AT&T and its Managing Agents. .... 19
    - 4. Mr. Terpin may Obtain Punitive Damages for Claims 5-7. .... 21
    - 5. This is Not a Case of First Impression. .... 21
- III. CONCLUSION ..... 23

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

**TABLE OF AUTHORITIES**

**CASES**

*Clayton v. Landsing Pac. Fund, Inc.*,  
2002 WL 1058247 (N.D.Cal. May 9, 2002), *aff'd*, 56 F. App'x 379  
(9th Cir. 2003) .....9

*Coll. Hosp. Inc. v. Superior Ct.*,  
8 Cal. 4th 704 (1999) ..... 18

*Cruz v. Homebase*,  
83 Cal. App. 4th 160 (2000)..... 13, 18

*Czuchaj v. Conair Corp.*,  
2014 WL 1664235 (S.D.Cal. April 18, 2014).....6

*Herron v. Best Buy Co. Inc.*,  
924 F. Supp. 2d 1161 (E.D.Cal. 2013) .....7

*Hodson v. Mars, Inc.*,  
891 F.3d 857 (9th Cir. 2018).....5, 6, 7

*In re First Alliance*,  
2003 WL 21430096 (C.D.Cal. June 16, 2003) .....22

*Johnson v. Riverside Healthcare Sys., LP*,  
534 F.3d 1116 (9th Cir. 2008)..... 11

*Lee v. City of Los Angeles*,  
250 F.3d 668 (9th Cir. 2001).....2

*Morgan Guar. Trust Co. v. American Sav. & Loan Ass'n*,  
804 F.2d 1487 (9th Cir. 1986).....22

*Perez v. Auto Tech. Co.*,  
2014 WL 12588644 (C.D.Cal. July 14, 2014).....19

*Razo v. TIMEC Co., Inc.*,  
2017 WL 5079249 (N.D.Cal. Nov 3, 2017) .....18

*Riggins v. Ortho McNeil Pharm. Inc.*,  
51 F. Supp. 3d 708 (N.D. Ohio 2014) .....9

*Smith v. Allstate Ins. Co.*,  
160 F. Supp. 2d 1150 (S.D. Cal. 2001) ..... 12

*Swartz v. KPMG LLP*,  
476 F.3d 756 (9th Cir. 2007)..... 11

*Tenzer v. Superscope, Inc.*,  
39 Cal. 3d 18 (1985) ..... 12

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 *UMG Recordings, Inc. v. Global Eagle Entertainment, Inc.*,  
117 F. Supp. 3d 1092 (C.D.Cal. 2015) ..... 11, 12

2

3 *Vess v. Ciba-Geigy Corp., USA*,  
317 F.3d 1097 (9th Cir. 2003)..... 11

4 *Weeks v. Baker & McKenzie*,  
63 Cal. App. 4th 1128 (1998)..... 18

5

6 **STATUTES**

7 47 U.S.C. § 222(a) ..... 14

8 Cal. Civ. Code § 3294(c)(1) ..... 19

9 Cal. Civ. Code § 3294(b) ..... 2, 3, 4, 17

10 Civ. Code § 3294(a)..... 17

11 Civ. Code § 3294(c)(3) ..... 20

12 Federal Communications Act, 47 U.S.C. §§ 206..... 6, 14, 15, 22

13 Federal Rules of Civil Procedure Rule 9(b)..... 11

14

15

16

17

18

19

20

21

22

23

24

25

26

27

28

1 **I. INTRODUCTION**

2 The motion to dismiss (“Motion”) Plaintiff’s Second Amended Complaint  
3 (“SAC”) of Defendant AT&T Mobility, LLC (“Defendant” or “AT&T”)  
4 inappropriately distorts the allegations made by Plaintiff Michael Terpin  
5 (“Plaintiff” or “Mr. Terpin”) in an improper attempt to dismiss Mr. Terpin’s fraud  
6 and punitive damages claims. The Motion should be denied.

7 First, Mr. Terpin has properly plead his third and fourth claims for relief for  
8 deceit by concealment and misrepresentation. AT&T virtually ignores the fact that  
9 Mr. Terpin has alleged that its representatives made *specific false representations* to  
10 Mr. Terpin after the first SIM swap on June 11, 2017 that were intended to induce  
11 him to continue being an AT&T customer, upon which he relied (to his very  
12 considerable detriment) and that are more than adequate to support his claims for  
13 deceit by concealment and misrepresentation. Moreover, one of AT&T’s primary  
14 arguments—that Mr. Terpin has not alleged more facts to support his fraud  
15 claims—is belied by the fact that AT&T alone is in possession of such facts and has  
16 delayed discovery that will reveal additional facts by bringing three successive  
17 motions to dismiss since this action was filed in August 2018.

18 Second, Mr. Terpin has properly plead punitive damages. AT&T’s attempt  
19 to strike the punitive damages claim similarly rests on a seemingly willful distortion  
20 of Plaintiff’s allegations regarding AT&T’s involvement in the SIM swaps alleged  
21 in the SAC. Mr. Terpin’s primary argument is that AT&T through its corporate  
22 officers and managing directors created an inadequate “security” system that  
23 allowed its employees and contractors to bypass controls to implement SIM swaps  
24 (either on their own or in conjunction with hackers from whom they accepted small  
25 bribes). In other words, Mr. Terpin is not “focus[ing]” (as AT&T alleges) on  
26 Jahmil Smith, but rather on the fact that AT&T knowingly and with deliberate  
27 disregard to the privacy of its customers put in place and maintained a highly  
28

1 inadequate security system that it knew could not prevent its own employees from  
 2 facilitating SIM swaps. *See* AT&T Motion to Dismiss FAC (“Motion”) at 8 n.3.

3 Further, especially in light of AT&T’s repeated assertions that Mr. Smith was  
 4 *not an AT&T* employee<sup>1</sup>, AT&T’s extensive reliance on cases under California  
 5 Civil Code Section 3294(b), which pertain to the ratification of acts of low-level  
 6 employees, is inapposite. Mr. Terpin has adequately alleged a basis for a claim for  
 7 punitive damages in the context of AT&T’s knowledge and obligations to protect  
 8 customer information, including its obligations to monitor and supervise its  
 9 employees under a prior consent decree from the Federal Communications  
 10 Commission (“FCC”) that dealt with precisely that issue. Mr. Terpin has further  
 11 alleged that AT&T and its officers and managing agents, including AT&T’s Chief  
 12 Compliance Officer and head of security, knew of the inadequacy of AT&T’s  
 13 security measures and deliberately disregarded and violated the rights of its  
 14 customers, including Mr. Terpin, all while continuing to falsely assure customers  
 15 that they could obtain a higher level of security by upgrading to a six-digit code.  
 16 As properly alleged in the SAC, AT&T is subject to punitive damages for Mr.  
 17 Terpin’s fraud and tort claims and AT&T’s motion to strike such damages should  
 18 be denied.

19 **II. ARGUMENT**

20 **A. Mr. Terpin Has Appropriately Alleged Deceit by Concealment.**

21 1. Mr. Terpin alleges that AT&T deceived him after the June 11,  
 22 2017 hack.

23 In his third claim for relief, Mr. Terpin alleges that AT&T knew its data  
 24 security system was grossly inadequate and that its employees could readily bypass  
 25

26 <sup>1</sup> AT&T has repeatedly made this assertion in its motions to dismiss, despite the  
 27 irrelevance of such factual assertions for such motion (defendant is bound to accept  
 28 the plaintiff’s allegations as true). *See, e.g., Lee v. City of Los Angeles*, 250 F.3d  
 668, 688 (9<sup>th</sup> Cir. 2001) (defendant’s factual assertions are irrelevant to a motion to  
 dismiss).

1 whatever protections it purported to give. SAC ¶¶ 143-145. This claim is further  
2 substantiated elsewhere in the SAC. For example, in Paragraph 78, Mr. Terpin  
3 alleges that an AT&T employee confirmed in an August 3, 2018 article in  
4 *Motherboard*, that “*the [AT&T] system is designed so that some employees have*  
5 *the ability to override security features such as the phone passcode that AT&T (and*  
6 *other companies) now require when porting numbers.* ‘From there the passcode  
7 can be changed,’ the employee said in an online chat, referring to a customer  
8 information portal that they showed *Motherboard*. ‘With a fresh passcode the  
9 number can be ported out with no hang ups.’” (Emphasis added.)

10 After Mr. Terpin’s initial SIM swap, he went on June 11, 2017 to an AT&T  
11 store in Puerto Rico to ask what additional security could be implemented on his  
12 account to prevent future hacks. SAC ¶ 88. As alleged in the SAC, “Mr. Terpin  
13 explained to AT&T that he had been hacked and that the hackers had stolen a  
14 substantial amount of money from him. Mr. Terpin expressed concern about  
15 AT&T’s ineffective security protections and asked how he could protect the  
16 security of his phone number and account against future unauthorized access,  
17 including hackers attempting to perpetrate SIM swap fraud.” *Id.*

18 As further alleged in the SAC:

19 [i]n response to Mr. Terpin’s request for greater security for his  
20 account and in order to induce Mr. Terpin to continue as an  
21 AT&T customer, AT&T promised that it would place his  
22 account on a “higher security level” with “special protection.”  
23 AT&T told Mr. Terpin that this “higher security level” would  
24 require anyone accessing or changing Mr. Terpin’s account to  
25 provide a six-digit passcode to AT&T to access or change the  
26 account. Anyone requesting AT&T to transfer Mr. Terpin’s  
27 telephone number to another phone must provide the code.  
28 AT&T promised Mr. Terpin at this meeting that the higher



1 security that it was placing on his account, which it also called  
2 “high risk” or “celebrity” protection, would ensure that Mr.  
3 Terpin’s account was much less likely to be subject to SIM  
4 swap fraud. AT&T further told Mr. Terpin that the  
5 implementation of the increased security measures would  
6 prevent Mr. Terpin’s number from being moved to another  
7 phone without Mr. Terpin’s explicit permission, because no  
8 one other than Mr. Terpin and his wife would know the secret  
9 code. AT&T made all of these promises to convince Mr.  
10 Terpin to continue to be an AT&T customer.

11 *Id.* See also SAC ¶¶ 143, 148, 150.

12 In inducing Mr. Terpin to stay with AT&T by promising that the “high risk”  
13 protection allegedly afforded by the additional six-digit Code would increase the  
14 security of his account, AT&T did not disclose that the additional security was  
15 worthless or ineffective because it could easily be bypassed or ignored by AT&T  
16 employees. ¶ 144. Specifically, AT&T “knew that its data security measures were  
17 grossly inadequate, that its employees and agents could readily bypass the  
18 procedures, that its employees actively cooperated with hackers and thieves, and  
19 that it was incapable of living up to its commitments to consumers, including to Mr.  
20 Terpin, under state and federal law, as well as under its own Privacy Policy, to  
21 protect his Personal Information, including CPI and CPNI.” SAC ¶ 143. AT&T  
22 made these false promises to induce Mr. Terpin to remain a customer. *Id.* Mr.  
23 Terpin believed AT&T’s promises and remained an AT&T customer. *Id.* ¶¶ 143,  
24 151.

25 The SAC also alleges that AT&T made the following false statements and/or  
26 omissions to Mr. Terpin:

- 27 (1) In June 2017, after the initial SIM swap, AT&T representatives  
28 encouraged Mr. Terpin to adopt additional security measures (adding a



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

- 1 six digit code) without telling Mr. Terpin that such security measures
- 2 could readily be evaded or bypassed by AT&T employees acting in
- 3 concert with individuals perpetrating SIM swap fraud;
- 4 (2) at all times herein relevant prior to the second SIM swap in January
- 5 2018, AT&T concealed the fact that its employees frequently acted in
- 6 concert with individuals perpetrating SIM swap fraud to provide such
- 7 individuals with personal information about its mobile users;
- 8 (3) at all times herein relevant prior to the second SIM swap in January
- 9 2018, AT&T concealed the fact that its employees frequently acted in
- 10 concert with individuals perpetrating SIM swap fraud to provide such
- 11 individuals with direct access to their customers’ accounts, which
- 12 enabled such individuals to intercept 2FA messages to customers; and
- 13 (4) because of the inadequacies of AT&T’s security measures and the active
- 14 participation of its employees in SIM swaps that AT&T’s promises in its
- 15 Privacy Policy had no value.

16 SAC ¶ 144.

17 2. AT&T Had a Duty to Disclose Material Facts.

18 AT&T alleges that Plaintiff’s Third Claim for Deceit by Concealment should  
19 be dismissed because defendant did not have a legal duty to disclose a material fact.  
20 AT&T’s argument is incorrect because three of the four circumstances set forth in  
21 *Hodson v. Mars, Inc.*, 891 F.3d 857, 862 (9<sup>th</sup> Cir. 2018), which it cites, existed in  
22 this case.

23 First, a duty arose because AT&T in fact had “exclusive knowledge of  
24 material facts” relating to its security system. Mr. Terpin had no way of knowing  
25 that the additional security precautions that AT&T was urging were not adequate.  
26 He accepted the affirmative statements that AT&T made after the June 11, 2017  
27 SIM swap and did not realize AT&T was hiding and concealing the true facts.

28 SAC ¶¶ 92, 143. Although Mr. Terpin was knowledgeable about cryptocurrency—

1 the SAC does not allege that he was an expert on security measures of  
 2 telecommunications providers, *id.* ¶ 18, nor is such an inference logical. Indeed, as  
 3 the SAC alleges, Mr. Terpin was only contacted by other victims of SIM swaps  
 4 *after* he filed the initial complaint in this action. See SAC ¶ 14 (“[s]ince the hack to  
 5 Mr. Terpin has occurred and this lawsuit has been filed, he has been contacted by  
 6 more than 50 SIM swap victims of AT&T, including many who had cryptocurrency  
 7 stolen under nearly identical circumstances”) (emphasis added).<sup>2</sup>

8 By contrast, AT&T is one of the world’s largest corporations and it and its  
 9 Chief Security Officer Bill O’Hern and Chief Compliance officer David Huntley  
 10 may fairly be presumed to have profound and superior knowledge about its security  
 11 system. *Id.* ¶ 75. Moreover, AT&T is legally required by the Federal  
 12 Communications Act (“FCA”), 47 U.S.C. §§ 206, 222 and an ongoing FCC  
 13 Consent Degree to protect its customers’ personal information, including protecting  
 14 it from being improperly accessed by its own employees. *Id.* ¶¶ 39-46, 51. Under  
 15 these circumstances AT&T undoubtedly had the “exclusive knowledge” sufficient  
 16 to give rise to a duty to speak

17 Secondly, AT&T also had a duty under *Hodson* to disclose material facts to  
 18 Mr. Terpin because it actively concealed material facts from Mr. Terpin.  
 19 Specifically, AT&T told Mr. Terpin on June 13, 2017 that he would be protected  
 20 against future SIM swaps by using the “higher” security afforded by a six digit code  
 21 but actively concealed the fact this security could be overridden or ignored by  
 22 AT&T employees. See SAC ¶¶ 11, 13, 77-79, 83, 89-94. AT&T’s concealment is  
 23 indeed an “affirmative act” directed to Mr. Terpin in which AT&T hid or concealed  
 24 its imperfect security. See *Czuchaj v. Conair Corp.*, 2014 WL 1664235, at \* 6  
 25 (S.D.Cal. April 18, 2014). AT&T’s active concealment consisted of its intentional

26 \_\_\_\_\_  
 27 <sup>2</sup> Similarly, all of the SIM swaps referenced in the SAC occurred *after* Mr. Terpin’s  
 28 SIM swap. See SAC ¶¶ 60-82. The only SIM Swap which is referenced in the  
 SAC that occurred *before* the January 2018 hack was that experienced by Mr.  
 Terpin on June 11, 2017. See SAC ¶¶ 88-89.

1 act in seeking to retain Mr. Terpin as a customer.

2 AT&T's statements after the June 11, 2017 are "partial representations" by  
 3 AT&T that were accompanied by "concealment of material facts" that also gave  
 4 rise to a duty to speak. *See Hodson* at 862 (quoted in the Motion at p. 5). The  
 5 "partial representations" are AT&T's statements regarding the efficacy of the six-  
 6 digit code. The "concealment" is AT&T's concealment of the fact that employees  
 7 could easily evade or bypass these protections, which in turn reveals the fallacy of  
 8 the assurances of higher security as a result of using the six-digit code. AT&T's  
 9 concealment certainly involves facts that would have "materially qualif[ied] the  
 10 facts disclosed or which render [AT&T's] disclosure likely to mislead." *Herron v.*  
 11 *Best Buy Co. Inc.*, 924 F. Supp. 2d 1161, 1177 (E.D.Cal. 2013). *See* SAC ¶ 161  
 12 ("Mr. Terpin would not have agreed to continue to use and pay for AT&T's  
 13 services if he had known that the additional security protection was ineffective and  
 14 that AT&T's other security measures were not as secure as represented by AT&T. .  
 15 . .")

16 AT&T is thus incorrect in stating that the "gravamen" of the SAC is the  
 17 inadequacy of AT&T's security system in and of itself. Mr. Terpin has multiple  
 18 claims and these concealment claims are grounded in the allegations that the  
 19 specific statements about heightened additional security, which were made to him  
 20 by AT&T after the June 11, 2017 hack, were inadequate and that AT&T made  
 21 material omissions regarding those statements to hide the inadequacy of its security  
 22 measures.

23 Mr. Terpin further provides adequate context for his allegations regarding the  
 24 falsity and incompleteness of AT&T's promises regarding the "higher level" six-  
 25 digit security. SAC ¶¶ 89-90. Based on information and investigations obtained by  
 26 Mr. Terpin, including information after his initial complaint was filed, Mr. Terpin  
 27 has alleged that AT&T employees frequently bypass or ignore its vaunted security  
 28 systems, including the additional code, because such security could be easily

1 overridden. For example, Mr. Terpin includes in his allegations statements by the  
 2 Santa Clara County REACT task force that telecommunication providers' security  
 3 is highly inadequate in preventing SIM fraud. SAC ¶ 74 (“someone needs to light a  
 4 fire under some folks [at the telecommunications providers] to get these protections  
 5 [to prevent SIM swap fraud] in place”). He further alleges that according to an  
 6 AT&T employee quoted in the August 3, 2018 *Motherboard* article that AT&T  
 7 employees can override security features including “the phone passcode that AT&T  
 8 (and other companies) now require when porting numbers” (SAC ¶ 78). Mr.  
 9 Terpin’s allegations thus provide more than adequate context for his allegations that  
 10 AT&T had a duty to disclose material facts to him when he met with AT&T after  
 11 the June 11, 2017 SIM swap.

12 AT&T’s argument that it disclosed (generally) in its Privacy Policy that it  
 13 does not “guarantee” security does not mean either that it had no duty to disclose  
 14 additional facts regarding security or provide AT&T from immunity particularly as  
 15 regards to the “higher level” security it convinced Mr. Terpin to place on his  
 16 account. The unremarkable statement that AT&T cannot “guarantee” security in no  
 17 way obviates Mr. Terpin’s allegation that he relied on the statements made  
 18 regarding a specific security measure that he was urged to place on his account,  
 19 particularly because AT&T told him that “anyone accessing or changing Mr.  
 20 Terpin’s account [would have] to provide a six-digit passcode to AT&T.” SAC  
 21 ¶ 89.<sup>3</sup> Unlike the cases cited in the Motion at p. 8, AT&T’s “warning” was highly  
 22 general and AT&T certainly did not reiterate the warning when it fought to keep  
 23 Mr. Terpin’s business by encouraging specific implementation of the “higher level”  
 24

---

25 <sup>3</sup> AT&T’s anodyne statement that it could not “guarantee” perfect security would  
 26 hardly have alerted Mr. Terpin to the fact that AT&T did not even have  
 27 rudimentary security to protect its own systems from misuse or that its employees  
 28 could readily evade or override its security measures. *See* SAC ¶ 58. *See also* ¶ 78  
 (AT&T employee cited to fact that AT&T employees could evade or override  
 security measures, including the “phone passcode that AT&T (and other  
 companies) now require when porting numbers.”

1 security through the six-digit code. This is therefore not a situation like that in  
 2 *Riggins v. Ortho McNeil Pharm. Inc.*, 51 F. Supp. 3d 708, 712 (N.D. Ohio 2014),  
 3 where the defendant disclosed dangers when it sold a product. Nor did AT&T in  
 4 fact “actually disclose” any information regarding the defects of the additional  
 5 security measures when it made statements regarding the “higher level” six-digit  
 6 code security on June 13, 2017. In contrast to *Clayton v. Landsing Pac. Fund, Inc.*,  
 7 2002 WL 1058247, at \*6 (N.D.Cal. May 9, 2002), *aff’d*, 56 F. App’x 379 (9<sup>th</sup> Cir.  
 8 2003), at the time the representations were made by AT&T to Mr. Terpin,  
 9 information regarding the inefficacy of the six-digit code was not readily found in  
 10 the market. Mr. Terpin’s allegations regarding the ease by which employees could  
 11 evade the security is based on information obtained after he was SIM swapped.

12 3. Mr. Terpin Has Adequately Plead that he was Unaware of  
 13 Concealed Material Facts.

14 AT&T is incorrect that Mr. Terpin has not adequately plead he was aware of  
 15 the concealed material facts. In the SAC, Mr. Terpin specifically alleges that he  
 16 was unaware that AT&T concealed that the additional security he was promised  
 17 after the June 11, 2017 hack (i.e., the six-digit passcode) was inadequate. SAC ¶  
 18 92. Moreover, he specifically alleges that if he had been aware that the additional  
 19 security was inadequate, that he would have left AT&T as his mobile carrier. *Id.*

20 It is risible for AT&T to claim that Mr. Terpin would have known that  
 21 AT&T’s six-digit code could be overridden or evaded by AT&T employees simply  
 22 by virtue of his involvement in cryptocurrency. Motion, p. 9. Moreover, as AT&T  
 23 itself acknowledges, Mr. Terpin was only contacted by other victims of AT&T’s  
 24 inadequate security practices *after* he filed his complaint in this action so that  
 25 information could not have put him on guard regarding AT&T’s fraud. Moreover,  
 26 for AT&T to claim that because Mr. Terpin had been victimized in the first SIM  
 27 swap that he should have known about the inadequacies of AT&T’s security is  
 28 astonishingly obtuse. Having been SIM swapped, Mr. Terpin was of course aware

1 of the practice. This is why he asked for (and was promised by AT&T) additional  
 2 security. In the event, AT&T did not disclose when he met with AT&T that the  
 3 additional security measures were worthless.

4 **B. Mr. Terpin Has Adequately Plead His Fourth Claim for Relief for**  
 5 **Misrepresentation.**

6 1. Mr. Terpin Adequately Alleges Reliance.

7 In his misrepresentation claim, Mr. Terpin alleges that “separate” from  
 8 representations and false promises made by AT&T in its Code of Business Conduct  
 9 and other documents that “an AT&T employee made specific promises to Mr.  
 10 Terpin after the June 11, 2017 hack regarding the security protection that would be  
 11 given to Mr. Terpin’s personal information by adding a six-digit security code on  
 12 the account. The AT&T employee did so in order to persuade Mr. Terpin not to  
 13 cancel his AT&T service.” SAC ¶ 159. Mr. Terpin further alleges that “AT&T  
 14 intended that Mr. Terpin rely on their representations and promises, including those  
 15 made after the June 11, 2017 hack, as it knew that Mr. Terpin would not entrust his  
 16 Personal Information to unreasonable security risks, particularly because Mr.  
 17 Terpin had been subject to the June 11, 2017 hack. In reliance upon AT&T’s  
 18 representations and promises, Mr. Terpin continued to maintain a wireless account  
 19 with AT&T and to use his AT&T phone number for verification and other  
 20 promises.” Id. ¶ 162.

21 Mr. Terpin thus clearly alleges “exposure” to statements by AT&T (in this  
 22 case in a face-to-face meeting with an AT&T representative in which the statements  
 23 were made), AT&T’s intent that Mr. Terpin rely on the representations (by  
 24 retaining him as an AT&T customer), and the fact that Mr. Terpin in fact did rely  
 25 on the representations (by continuing to be an AT&T customer). SAC ¶ 92. Thus,  
 26 even if the Court were to find that Mr. Terpin has not alleged adequate reliance on  
 27 documents referenced in the SAC, the Fourth Claim for Relief should still proceed  
 28 on the basis that AT&T made representations to him regarding its security measures



1 after the June 11, 2017 hack on which he relied. *See Johnson v. Riverside*  
 2 *Healthcare Sys., LP*, 534 F.3d 1116, 1121-22 (9<sup>th</sup> Cir. 2008) (to survive a motion to  
 3 dismiss compliant must present cognizable legal theories and sufficient allegations  
 4 to support those theories).

5 2. Mr. Terpin has Adequately Alleged that AT&T's statements  
 6 were known to be false.

7 AT&T additionally argues that the claim should be dismissed because Mr.  
 8 Terpin has not adequately alleged that AT&T did not intend to ignore the  
 9 heightened security protocol and that all Mr. Terpin has alleged is that AT&T did  
 10 not perform its promise. In making this argument, AT&T—for the first time after  
 11 two prior rounds of motion practice—claims under Rule 9(b) of the Federal Rules  
 12 of Civil Procedure that Mr. Terpin's claim is not plead with particularity (without  
 13 expressly stating that it is doing so).

14 Mr. Terpin's claims pass muster under Rule 9(b) because AT&T  
 15 undoubtedly has notice of the "particular misconduct so that [it] can defend against  
 16 the charge[.]." *Vess v. Ciba-Geigy Corp., USA*, 317 F.3d 1097, 1006 (9<sup>th</sup> Cir. 2003).  
 17 AT&T has knowledge from the SAC of the representations that were made to Mr.  
 18 Terpin (regarding six-digit "higher level" security), the date of those representations  
 19 (June 13, 2017), the location (a Puerto Rico AT&T store), and the statements made  
 20 by the AT&T representative at that meeting. *Swartz v. KPMG LLP*, 476 F.3d 756,  
 21 764 (9<sup>th</sup> Cir. 2007).

22 Defendant's claim that Mr. Terpin has not adequately alleged that AT&T did  
 23 not intend to perform its promise can also be expressed as whether AT&T's  
 24 statements were "false when made." *See UMG Recordings, Inc. v. Global Eagle*  
 25 *Entertainment, Inc.*, 117 F. Supp. 3d 1092, 1108 (C.D.Cal. 2015) ("plaintiff must  
 26 plead facts explaining why the statement was false when made" (quoting *Smith v.*  
 27 *Allstate Ins. Co.*, 160 F. Supp. 2d 1150, 1152 (S.D. Cal. 2001)). At the pleading  
 28 stage of a promissory fraud claim, the determination of this question only "requires



1 pleading facts from which it can be inferred that the promisor had no intention of  
2 performing at the time the promise was made.” *Id.*

3 Mr. Terpin here alleges more than mere non-performance. He alleges that  
4 AT&T “did not intend to perform either its promises in the Privacy Policy or after  
5 the June 11, 2017 hack regarding the security protection that would be given to Mr.  
6 Terpin’s personal information by adding a six-digit security code on the account.”  
7 SAC ¶159. The reason why AT&T did not intend to perform its promises was  
8 because AT&T “knew that is security protections, including the six-digit security  
9 code were ineffectual and could easily be evaded or bypassed by its employees.”  
10 SAC ¶ 160. Mr. Terpin also alleges that such “representations and promises were .  
11 . . false because AT&T was using outdated security procedures and failed to  
12 disclose that it did not adhere to its own standards. . . .” *Id.* AT&T further knew  
13 that the statements were false because it knew “it did not have in place state-of-the  
14 art security protections, such as a SIM lock out.” *Id.*

15 As in *Tenzer v. Superscope, Inc.*, 39 Cal. 3d 18, 30-31 (1985), AT&T’s  
16 fraudulent intent can be inferred by the facts and circumstances alleged in the SAC,  
17 including its knowledge that its employees could easily evade the protections (as  
18 shown in statements by an AT&T employee in the *Motherboard* article). Under  
19 these circumstances Mr. Terpin has properly alleged that AT&T knew that its  
20 promise that such a security standard would protect Mr. Terpin was false when  
21 made.<sup>4</sup>

22 Moreover, Mr. Terpin is not alleging that AT&T failed to “guarantee”  
23 security, that its promises were “overly optimistic,” or that AT&T had an “honest  
24

25 <sup>4</sup> The standard for false representations is that they are “false” when made. Falsity  
26 can be expressed as the falsity of the statements themselves. *See Smith v. Allstate*  
27 *Ins. Co.*, 160 F. Supp. 2d 1150, 1153-54 (S.D.Cal. 2001), *cited* in the Motion p. 12  
28 (plaintiff must “plead facts explaining why the statement was false when it was  
made”). In this case, AT&T’s statements regarding the security procedures were  
false not simply because AT&T did not keep its promises, but also because the  
statements themselves were intrinsically false.

1 but unreasonable intent to perform.” Motion, p. 13. Instead, Mr. Terpin is alleging  
 2 that AT&T promoted a security protocol that afforded no real security because it  
 3 knew that it could be evaded or overridden by its employees. AT&T knew that  
 4 even after AT&T placed the six-digit code on Mr. Terpin’s account that this would  
 5 not prevent employees from overriding or ignoring the protocol. AT&T’s  
 6 statements to Mr. Terpin after the June 11, 2017 hack were thus demonstrably false.

7 **C. Mr. Terpin Has Properly Alleged Punitive Damages.**

8 1. Mr. Terpin’s Alleges Punitive Damages Based on the Actions of  
 9 AT&T’s Officers and Managing Agents.

10 AT&T’s motion to strike punitive damages distorts the allegations of the  
 11 SAC. Mr. Terpin’s claim for punitive damages arises from the direct actions of  
 12 AT&T undertaken through its officers and management—not from the actions of a  
 13 single individual (Jahmil Smith).<sup>5</sup> As the SAC alleges, AT&T consciously and  
 14 maliciously put in place a system that it knew would not protect the security and  
 15 privacy of its customers’ personal information. As the SAC further alleges, the  
 16 “higher level” security measures that AT&T urged Mr. Terpin to adopt after the  
 17 first SIM swap on June 11, 2017 were known to AT&T to be ineffectual because  
 18 they could readily be bypassed or overridden by AT&T employees. SAC ¶¶ 89-92.  
 19 AT&T is thus subject to punitive damages not because of the actions of the  
 20 individual who is believed to have turned over the information, but because its  
 21 corporate managerial employees knowingly implemented and maintained a system  
 22 that did not protect the private information and communications of its customers.  
 23 *See Cruz v. Homebase*, 83 Cal. App. 4<sup>th</sup> 160, 167 (2000) (award of punitive  
 24 damages against a corporation rests on proof of malice of corporate leaders (citing  
 25 Cal. Civ. Code § 3294(b)).

26 \_\_\_\_\_  
 27 <sup>5</sup> Mr. Terpin has alleged claims for negligent supervision and training and negligent  
 28 hiring (sixth and seventh claims for relief) that may implicate AT&T’s actions in  
 regard to employees (or contractors) like Mr. Smith and his employer Spring  
 Communications. *See* Motion, p. 8, n. 3.

1 a. AT&T Has Violated Its Obligations Under Law By  
 2 Allowing Its Employees to Turn Over its Customers'  
 3 Personal Information.

4 AT&T was well aware of its obligations to protect its customers' personal  
 5 information and equally well aware that its security systems were inadequate.  
 6 AT&T had an obligation under Section 222(a) of the FCA, 47 U.S.C. § 222(a), to  
 7 protect the confidential information of its customers. SAC ¶¶ 28-34. Under the  
 8 FCC's CPNI Rules implementing the FCA, AT&T was required to establish  
 9 measures to prevent the disclosure of CPNI by employees to unauthorized  
 10 individuals, including presentation of adequate means of identification by  
 11 customers to AT&T. SAC ¶ 34.

12 Moreover, the SAC alleges that AT&T and its corporate officers were put on  
 13 notice regarding its employees' disclosure of its customers' personal information  
 14 through the April 8, 2015 FCC Consent Decree and were required to remedy the  
 15 deficiencies in AT&T's security, hiring and training practices. *See* SAC ¶¶ 39-51.  
 16 In conjunction with a pretexting scam, the FCC fined AT&T a record \$25 million  
 17 for violating Section 222 of the FCA by allowing its employees to hand over to  
 18 thieves the personal information of almost 280,000 customers. *Id.* ¶ 39. In the  
 19 consent decree of the same date ("Consent Decree") (which remains in full force  
 20 and effect), the FCC cited (i) AT&T's lax security practices; (ii) the fact that  
 21 employees were paid by criminals to hand over AT&T customers' personal  
 22 sensitive information; (iii) the further fact that AT&T employees readily breached  
 23 AT&T's security; and (iv) AT&T's failure properly to supervise its employees. *Id.*  
 24 ¶¶ 40-43.

25 In the Consent Decree the FCC ordered AT&T to (i) take "every reasonable  
 26 precaution" to protect customers' data; (ii) imposed obligations on AT&T to  
 27 properly manage and supervise employees; (iii) required AT&T to designate "a  
 28 senior corporate manager with the requisite corporate and organization authority to

1 serve as a Compliance Officer; and (iv) required the company to implement a  
 2 “Compliance Plan” including an “Information Security Program,” “Ongoing  
 3 Monitoring and Improvement,” and a “Compliance Review.” *Id.* ¶¶ 44-47. The  
 4 “Information Security Program” required under the Consent Decree specifically  
 5 required AT&T to implement “*access controls reasonably designed to limit access*  
 6 *to Personal Information and CPNI to authorized AT&T employees, agents, and*  
 7 *Covered Vendor Employees.*” ¶ 48 (emphasis added).

8 b. AT&T’s Corporate Officers Deliberately Perpetuated A  
 9 Grossly Inadequate Security System.

10 AT&T and its corporate officers Bill O’Hern, who has been AT&T’s Chief  
 11 Security Officer and headed AT&T’s security operations since 2016, and David S.  
 12 Huntley, AT&T’s Executive Vice President & Chief Compliance Officer, are  
 13 presumptively well aware of AT&T’s security system and the requirements of the  
 14 Consent Decree as pertains to employees protecting customers’ personal  
 15 information. SAC ¶ 75. Indeed, Mr. Huntley (who bears the “Compliance Officer”  
 16 title referenced in the Consent Decree) is responsible at AT&T for “verifying  
 17 compliance with legal and regulatory requirements of the countries and  
 18 jurisdictions where AT&T operates, and ensuring adherence to internal compliance  
 19 standards.” *Id.*, citing <https://investors.att.com/corporate-governance/leadership>.  
 20 These compliance standards likely include adherence to the requirements of the  
 21 Consent Decree.

22 The SAC thus alleges that AT&T deliberately ignored the requirements of  
 23 the Consent Decree by establishing and continuing to promote to its customers a  
 24 system that it knew did not protect customers’ information. Moreover, AT&T,  
 25 acting through executives like Messrs. O’Hern and Huntley, did nothing to prevent  
 26 AT&T employees from turning over that information to hackers in SIM swaps.  
 27 SAC ¶ 109. The SAC further alleges that AT&T’s corporate officers, including  
 28 Messrs. O’Hern and Huntley, knew that AT&T’s security system was inadequate,

1 knew that its employees could readily bypass or ignore the system, and that its  
 2 employees were susceptible to bribes to turn information over to hackers. SAC  
 3 ¶¶ 75, 77-79, 83-84, 90-93, 143-45, 149, 156.

4 Mr. Terpin discovered the manifest deficiencies of the system to his peril  
 5 when an AT&T employee turned over his information to hackers, despite the  
 6 vaunted “higher level” security that AT&T had placed on his account. As a result  
 7 of the disclosure of personal information and communications, Mr. Terpin lost over  
 8 \$24 million in cryptocurrency.

9 c. The SAC Adequately Alleges that Employees Can  
 10 Readily Evade or Bypass AT&T’s Security System.

11 Although he has not had the benefit of discovery from AT&T, Mr. Terpin  
 12 has substantiated his allegations against AT&T with information about other SIM  
 13 swaps involving AT&T employees and media stories about the security of AT&T  
 14 and other telecommunications carriers. *See, e.g.*, SAC ¶¶ 73-74 (REACT task force  
 15 cites store employees’ involvement in SIM swaps because of carriers’ inadequate  
 16 security); ¶ 76 (carriers are “weakest link” in security according to authors of article  
 17 in *bitcoinist.com*); ¶78 (*Motherboard* article quotes AT&T employee as stating that  
 18 AT&T doesn’t have sufficient safeguards to stop employees and that the AT&T  
 19 “system is designed so that some employees have the ability to override security  
 20 features such as the phone passcode that AT&T (and other companies) now require  
 21 when porting numbers”).

22 The pattern that emerges from these reports is similar to the pretexting cases  
 23 that led to the FCC’s Consent Decree. As reported by both insiders and law  
 24 enforcement, AT&T employees are readily bribed to turn over the personal  
 25 information of its customers to hackers, who use that information to commit SIM  
 26 swaps. SAC ¶¶ 9, 67, 73. Ignoring the Consent Decree (and apparently not  
 27 deterred by a \$25 million fine), AT&T and its corporate officers are again  
 28 maintaining a system that does nothing to prevent employees from turning over its

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

1 customers’ personal information and communications. Moreover, as the SAC  
2 alleges, AT&T and its officers and managers have not put in place measures, such  
3 as a SIM lockdown, that would provide further protection of its customers’  
4 information and communications. SAC ¶¶ 14, 143.

5 2. Cases Involving the Ratification of the Actions of Low-Level  
6 Employees are Not Relevant.

7 Unlike many of the cases cited by AT&T, this is not a case where corporate  
8 officers’ knowledge of a specific lower level employee charged with wrongful  
9 conduct (such as sexual harassment or stalking) provides a basis for punitive  
10 damages through ratification of the employee’s actions. Instead, the gravamen of  
11 Mr. Terpin’s allegations is that the actions of AT&T’s corporate officers and  
12 managing agents were malicious, oppressive and fraudulent.

13 Under Civil Code § 3294(a), “[i]n an action for the breach of an obligation  
14 not arising from contract, where it is proven by clear and convincing evidence that  
15 the defendant has been guilty of oppression, fraud, or malice, the plaintiff, in  
16 addition to the actual damages, may recover damages for the sake of example and  
17 by way of punishing the defendant.”

18 Civil Code § 3294(b) further provides that “[a]n employer shall not be liable  
19 for damages pursuant to subdivision (a), based upon acts of an employee of the  
20 employer, unless the employer had advance knowledge of the unfitness of the  
21 employee and employed him or her with a conscious disregard of the rights or  
22 safety of others or authorized or ratified the wrongful conduct for which the  
23 damages are awarded or was personally guilty of oppression, fraud, or malice. With  
24 respect to a corporate employer, the advance knowledge and conscious disregard,  
25 authorization, ratification or act of oppression, fraud, or malice must be on the part  
26 of an officer, director, or managing agent of the corporation.”

27 In order to impose punitive damages on a corporation, California’s “punitive  
28 damages statute requires proof of malice among corporate leaders: the ‘officer[s],



1 director[s], or managing agent[s].” *Cruz*, at 166. “Managing agents” are  
 2 “employees who ‘exercise [] substantial discretionary authority over decisions that  
 3 ultimately determine corporate policy.’” *Id.*, quoting *White v. Ultramar*, 21 Cal.  
 4 4<sup>th</sup> 563, 577 (1999). The purpose of punitive damages is to punish malice “among  
 5 corporate leaders” who “guide corporate conduct” and to “avoid[] punishing the  
 6 corporation for malice of low-level employees which does not reflect the corporate  
 7 ‘state of mind’ or the intentions of corporate leaders.” *Cruz*, 83 Cal. App. 4<sup>th</sup> at  
 8 167.

9 Many of the cases cited by AT&T are irrelevant to the allegations of the SAC  
 10 because they involve the issue of whether a corporation through its managing  
 11 agents ratified the conduct of a lower level employee. For example, in *Weeks v.*  
 12 *Baker & McKenzie*, 63 Cal. App. 4<sup>th</sup> 1128, 1154 (1998) the issue was whether a law  
 13 firm was liable for the actions of an employee because an “officer, director or  
 14 managing agent” had knowledge of the unfitness of the employee and employed  
 15 him with the conscious disregard of the safety of others. *See* Motion, p. 15.  
 16 Similarly, in *Coll. Hosp. Inc. v. Superior Ct.*, 8 Cal. 4<sup>th</sup> 704, 726 (1999) the issue  
 17 related to an employer’s ratification of an employee’s misconduct. *See also Razo v.*  
 18 *TIMEC Co., Inc.*, 2017 WL 5079249, at \*19 (N.D.Cal. Nov 3, 2017) (lack of  
 19 knowledge of executives of an unfit employee. These cases (and similar cases cited  
 20 by AT&T) are not applicable here because Mr. Terpin is alleging that AT&T  
 21 directly engaged in despicable conduct by setting “corporate policy” through its  
 22 officers, directors and managing agents, not that it ratified the actions of Jahmil  
 23 Smith. *See Cruz, supra*, at 167-168.

24 Contrary to AT&T’s implication, Mr. Terpin did not pull the names of Mr.  
 25 O’Hern and Mr. Huntley out of a hat. Based on publicly available information,  
 26 these are precisely the individuals at AT&T who are responsible for setting  
 27 AT&T’s corporate policy regarding security and privacy matters. SAC ¶¶ 75, 77-  
 28 79, 83-84, 90-93, 143-45, 149, 156. Although Mr. Terpin has not had the benefit of



1 discovery to uncover the exact mechanics of AT&T’s implementation of its  
 2 ineffective security program, Mr. Huntley is the Chief Compliance Officer of  
 3 AT&T (and thus was called upon in the FCC’s Consent Decree to implement  
 4 improvements to AT&T’s security system necessary to prevent its employees from  
 5 turning over the personal information of its customers). According to publicly  
 6 available information, Mr. Huntley is also responsible for regulatory compliance  
 7 and privacy at AT&T. See SAC ¶ 75, citing [https://investors.att.com/corporate-](https://investors.att.com/corporate-governance/leadership)  
 8 [governance/leadership](https://investors.att.com/corporate-governance/leadership) (article on David S. Huntley). Mr. O’Hern is also named  
 9 because he is in charge of security at AT&T and is thus charged with making sure  
 10 that customers’ information is secure. SAC ¶ 75, citing  
 11 <https://about.att.com/innovationblog/030116billohern> (article on Bill O’Hern). In  
 12 any event, AT&T’s assertions on this issue are not properly addressed at the  
 13 pleading stage.

14           3.     Mr. Terpin Has Adequately Alleged Malice, Oppression and  
 15                   Fraud by AT&T and its Managing Agents.

16           AT&T further argues that Mr. Terpin has not plead the requisite mental state  
 17 of its officers and managing agents. This argument rests on the same  
 18 misconception as its first argument, *i.e.*, that the requisite mental state relates to  
 19 such officers’ knowledge regarding a single individual (Mr. Smith) as opposed to  
 20 the mental state of the executives and managing agents themselves as to AT&T’s  
 21 inadequate security program. In that regard, Mr. Terpin has indeed specifically  
 22 alleged facts, including “conduct that is both willful and despicable” and that  
 23 “subjects a person to cruel and unjust hardship in conscious disregard of that  
 24 person’s rights.” Motion, p. 19, quoting *Lackner v. North*, 135 Cal. App. 4<sup>th</sup> 1188,  
 25 1211, 1213 (2006); *Perez v. Auto Tech. Co.*, 2014 WL 12588644 (C.D.Cal. July 14,  
 26 2014). See also Cal. Civ. Code § 3294(c)(1) (defining malice (in part) as “conduct  
 27 which is carried on by the defendant with a willful and conscious disregard of the  
 28 rights of others”); § 3294(c)(2) (defining oppression as “despicable conduct that

1 subjects a person to cruel and unjust hardship in conscious disregard of that  
 2 person’s rights”) and § 3294(c)(3) (defining fraud as “intentional misrepresentation,  
 3 deceit or concealment of a material fact known to the defendant with the intention  
 4 on the part of the defendant of thereby depriving a person of property or legal rights  
 5 or otherwise causing injury”).

6 Mr. Terpin alleges that AT&T, despite its knowledge that its employees had  
 7 betrayed the privacy of customer accounts previously and its obligation under the  
 8 Consent Decree to institute a security program that would prevent its employees  
 9 from turning over customer information to third parties, consciously and  
 10 deliberately established a security system that it knew could be overridden or  
 11 ignored by employees to turn over customer information to hackers for SIM swaps.  
 12 The SAC further alleges that AT&T did not properly hire, monitor or supervise its  
 13 employees (despite its obligation to do so under the Consent Decree). Moreover,  
 14 AT&T consciously and deliberately violated the promises that it made in its privacy  
 15 policies about protecting customers’ information by encouraging Mr. Terpin after  
 16 the June 11, 2017 SIM swap to implement a six-digit code that it knew could easily  
 17 be evaded or overridden by its employees. These allegations are substantiated by  
 18 statements by law enforcement and an AT&T employee. SAC ¶¶ 73-74, 77-78.  
 19 These actions are not only malicious and oppressive, but also constitute fraud.  
 20 Indeed, Mr. Terpin in his third and fourth claims for relief allege the elements of  
 21 both claims for misrepresentation and false promise involving the acts of AT&T  
 22 officers and managing agents. Such actions undoubtedly are fraud under Civil  
 23 Code § 3294(c)(3).

24 AT&T is incorrect that the SAC merely contains “conclusory allegations.”  
 25 As outlined above, the SAC contains detailed allegations replete with context and  
 26 citations to other sources substantiating a pattern on the part of AT&T and its  
 27 employees. Contrary to AT&T’s unsupported charge, the inferences that Mr.  
 28 O’Hern and Mr. Huntley were knowledgeable and were involved in the corporate

1 policy is established by their roles in the company as stated in AT&T’s public  
 2 materials. Indeed, Mr. Huntley as AT&T’s “Compliance Officer” is charged with  
 3 protecting customers’ personal information. See SAC ¶¶ 46, 56 and 75. Because of  
 4 their roles and responsibilities, Messrs. O’Hern and Huntley are charged with  
 5 knowledge of the security lapses that led employees to divulge personal information  
 6 to third parties to facilitate SIM swaps and AT&T’s obligations to comply with its  
 7 responsibilities to protect customers’ personal information.

8 4. Mr. Terpin may Obtain Punitive Damages for Claims 5-7.

9 AT&T further alleges that punitive damages are not available for Mr.  
 10 Terpin’s claims for negligence, negligence supervision, and negligent hiring.  
 11 AT&T cites no authority for striking the punitive damages for these claims at this  
 12 stage prior to discovery. The unremarkable principle that punitive damages may  
 13 not be based on mere negligence is a principle that applies to an award of punitive  
 14 damages *at trial*—not striking the claims at the pleading stage before discovery has  
 15 even commenced.

16 As the SAC alleges, the Consent Decree called upon AT&T to remediate its  
 17 hiring, training and retention policies of employees to prevent employees turning  
 18 over customers’ personal information to unauthorized third parties. SAC ¶¶ 40-51.  
 19 If it is shown at trial that AT&T’s officers and other managing agents knew that it  
 20 continued to engage in defective hiring, training and retention policies and that such  
 21 actions were undertaken with malice, fraud or oppression (as alleged in the SAC),  
 22 Mr. Terpin may be entitled to punitive damages for these claims, as well as the  
 23 claims alleging fraud. This, however, is a matter not for a motion to dismiss,  
 24 because it involves factual issues.

25 5. This is Not a Case of First Impression.

26 The fact that this case involves SIM swapping (instead some other form of a  
 27 security breach) is not a ground for dismissing the prayer for punitive damages at  
 28 the pleading stage. Although the facts of this case (as with many other cases) may

1 involve some unique elements, the legal issues are not unique, i.e., AT&T's  
 2 liability for actions that it undertook that exposed Mr. Terpin's personal  
 3 information in violation of his rights.

4 The rationale for the rule that punitive damages may not be appropriate in  
 5 cases of first impression is that "the requisite intent or willfulness required to  
 6 consciously disregard another's rights cannot be present if no right or duty has been  
 7 recognized." *In re First Alliance*, 2003 WL 21430096, at \*10 (C.D.Cal. June 16,  
 8 2003). Because punitive damages must be based on conscious disregard of  
 9 another's rights, the Ninth Circuit in a "close case" found that they were not  
 10 appropriate where there not a clear tenable claim of right. *Morgan Guar. Trust Co.*  
 11 *v. American Sav. & Loan Ass'n*, 804 F.2d 1487, 1500 (9<sup>th</sup> Cir. 1986).

12 In contrast, the rights at issue in this case are well established and  
 13 recognized. Mr. Terpin as an AT&T customer had a statutory right for protection  
 14 of his personal information and communications under the FCA and AT&T had the  
 15 obligation to protect that information. SAC ¶¶ 28-32. Indeed, the FCA gives Mr.  
 16 Terpin a private right of action to enforce those rights under the FCA and he is  
 17 seeking to do so in this action. SAC ¶¶ 133-141. Mr. Terpin's rights are further  
 18 based on the CPNI Rules that require carriers like AT&T to implement measures to  
 19 prevent disclosure of personal information to unauthorized individuals. SAC ¶¶ 32-  
 20 34. Moreover, the FCC enforced consumers' rights to the privacy of personal  
 21 information against AT&T in the pretexting cases and through the resulting  
 22 Consent Decree. In those cases, as here, AT&T inadequately protected its  
 23 customers' personal information from being turned over to criminals by its  
 24 employees. SAC ¶¶ 35-51. AT&T itself acknowledges these rights in its Privacy  
 25 Policy and Code of Business Conduct. SAC ¶ 52 *et seq.* For example, in its  
 26 Privacy Policy, AT&T states that it takes its responsibility to safeguard customers'  
 27 personal information "seriously" and that it will not share such information except  
 28 for legitimate business purposes. *Id.* ¶ 54. It also promises that it has safeguards in

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

place to protect such information, including safeguards as to how its employees protect such information. *Id.* ¶ 55.

Under these circumstances, there is nothing novel about the rights at issue in this case. Nor, unfortunately, is there anything novel about the fact that AT&T did not have safeguards in place to protect the security of Mr. Terpin’s information from the actions of its own employees, given that it was fined \$25 million in 2015 for similar actions. Under the rationale of *In re First All Mortg.*, the rights and duties involved here are well-established and can readily serve as a basis for a punitive damages claim based on AT&T’s malicious flaunting of those rights in the case of Mr. Terpin.

Moreover, as the foregoing discussion shows, there are—at a minimum—disputed facts as to AT&T’s claim that this case is sufficiently “novel” so as to avoid punitive damages that would make it improper to strike these allegations at the pleading stage and without allowing Mr. Terpin the benefit of discovery.

**III. CONCLUSION**

For the foregoing reasons, the Court should deny Defendant’s Motion to Dismiss Third and Fourth Claims for Relief and Mr. Terpin’s claim for punitive damages. Alternatively, Mr. Terpin seeks leave to amend such claims.

DATED: April 13, 2020

GREENBERG GLUSKER FIELDS  
CLAMAN & MACHTINGER LLP

By: /s/ Pierce O’Donnell  
PIERCE O’DONNELL (SBN 081298)  
Attorneys for Plaintiff MICHAEL  
TERPIN