FOR PUBLICATION

UNITED STATES COURT OF APPEALS
FOR THE NINTH CIRCUIT

MICHAEL TERPIN, *Plaintiff-Appellant*, v. AT AND T MOBILITY LLC, *Defendant-Appellee*, and DOES, 1-10, *Defendant*.	No.23-55375 D.C. No. 2:18-cv-06975- ODW-KS OPINION

Appeal from the United States District Court
for the Central District of California
Otis D. Wright II, District Judge, Presiding

Argued and Submitted March 8, 2024
Pasadena, California

Filed September 30, 2024

Before: Richard R. Clifton, Holly A. Thomas, and Roopali H. Desai, Circuit Judges.

Opinion by Judge Desai

SUMMARY*

Federal Communications Act / California State Law

The panel affirmed the district court's dismissal of some claims and affirmed in part and reversed in part the district court's grant of summary judgment for mobile service provider AT&T Mobility, LLC, on the remaining claims brought by Michael Terpin after hackers gained control over his phone number through a fraudulent "SIM swap," received password reset messages for his online accounts, and stole $24,000,000 of his cryptocurrency.

Terpin sued AT&T under the Federal Communications Act and California state law for failing to adequately secure his account. Affirming the district court's dismissal of Terpin's fraud claims and punitive damages claim, the panel held that he failed to state a claim for deceit by concealment because he did not allege that AT&T had a duty to disclose regarding extra security that it promised him. Terpin failed to state a claim for fraudulent misrepresentation because he did not allege that AT&T made a promise with intent to perform. And he failed to allege facts sufficient to support punitive damages.

The panel affirmed the district court's summary judgment on Terpin's claim for AT&T's breach of the Privacy Policy incorporated in its Wireless Customer Agreement. Terpin sought consequential damages for the loss of his cryptocurrency to hackers, but the panel held that

* This summary constitutes no part of the opinion of the court. It has been prepared by court staff for the convenience of the reader.

consequential damages were barred by the limitation of liability clause in the parties' agreement.

Affirming the district court's summary judgment on Terpin's negligence claims, the panel held that these claims were foreclosed by the economic loss rule, which bars claims between contractual parties when the claims arise from or are not independent of the parties' underlying contracts.

The panel reversed the district court's summary judgment and remanded on Terpin's claim under Section 222 of the Federal Communications Act, which provides that telecommunications carriers have a duty to protect "customer proprietary network information," or "CPNI." Declining to address whether Section 222 protects both CPNI and a broader category of customer proprietary information, or only CPNI, the panel held that Terpin created a triable issue over whether, through the fraudulent SIM swap, AT&T gave hackers access to information protected under the Act.

COUNSEL

Pierce H. O'Donnell (argued), Timothy J. Toohey, Paul A. Blechner, and Emily Avazian, Greenberg Glusker Fields Claman & Machtinger LLP, Los Angeles, California, for Plaintiff-Appellant.

Marcellus A. McRae (argued), Gibson Dunn & Crutcher LLP, Los Angeles, California; Allyson N. Ho, Ashley E. Johnson, and Michael A. Zarian, Gibson Dunn & Crutcher LLP, Dallas, Texas; Jeremy Ochsenbein, Gibson Dunn & Crutcher LLP, Denver, Colorado; Nancy L. Stagg, Kilpatrick Townsend & Stockton LLP, San Diego, California; for Defendant-Appellee.

Megan Iorio, Christopher Frascella, and Tom McBrien, Electronic Privacy Information Center, Washington, D.C., for Amici Curiae Electronic Privacy Information Center and National Consumers League.

Joshua S. Turner, Sara M. Maxenberg, and William Turner, Wiley Rein LLP, Washington, D.C., for Amicus Curiae CTIA – The Wireless Association.

OPINION

DESAI, Circuit Judge:

Plaintiff Michael Terpin sued his mobile service provider, AT&T Mobility LLC ("AT&T"), after hackers gained control over his phone number through a fraudulent "SIM swap," received password reset messages for his online accounts, and stole $24,000,000 of his cryptocurrency. Terpin alleges AT&T engaged in fraud and negligence and breached its contractual and statutory duties by failing to secure Terpin's account. The district court dismissed some of Terpin's claims for failure to state a claim and later entered summary judgment against him on his remaining claims. We affirm the district court's dismissal of Terpin's fraud claims and punitive damages claim, and we affirm in part and reverse in part the district court's grant of summary judgment for AT&T on Terpin's remaining claims.

Background

Terpin is a well-known cryptocurrency investor. Cryptocurrency is accessed through digital "wallets" by entering an owner's access credentials. The wallet is an application that holds the private keys necessary to access or transact cryptocurrency.

Terpin contracted with AT&T for his cell phone service in 2011. The parties' relationship was governed by the "Wireless Customer Agreement," which incorporated the "Privacy Policy."

In 2017, Terpin was a victim of a "SIM swap" scam involving his AT&T account. A "SIM" ("subscriber identity module") is a microchip that connects a phone or other

device to a cellular network. The cellular network uses SIM identification information to associate the device with a phone number and customer account so it can route communications and tie wireless services to the customer's account. A "SIM swap" happens when a phone number associated with one SIM becomes associated with a different SIM. No information on the old SIM is transferred to the new SIM, but the new SIM becomes tied to the account and receives all new incoming calls and messages. Terpin alleges that hackers impersonated him to conduct a SIM swap in June 2017 and he lost some cryptocurrency as a result. That SIM swap is not at issue here.

About two months after the 2017 SIM swap, Terpin alleges he met with AT&T "representatives" to discuss ways to prevent future SIM swap fraud. Terpin alleges that AT&T promised him "extra security" by requiring him to provide a six-digit code rather than a four-digit code to make changes to his account.

In 2018, Terpin was the victim of another fraudulent SIM swap. That SIM swap gave rise to this lawsuit. The teenage perpetrator, Ellis Pinsky, bribed an employee at an AT&T authorized retailer, Jahmil Smith, to bypass AT&T's security measures and "swap" Terpin's phone number to a SIM Pinsky and his associate controlled. After the swap, Pinsky requested password reset messages to Terpin's phone number and used those messages to gain access to Terpin's online accounts, including a Microsoft OneDrive account. Pinsky searched Terpin's OneDrive and found a document in the trash folder with Terpin's cryptocurrency access credentials. Pinsky used those credentials to access Terpin's "wallets" and steal $24 million in cryptocurrency.

Procedural History

Terpin sued AT&T for failing to adequately secure his account.[1] After multiple rounds of motions to dismiss, Terpin filed a second amended complaint. It included one federal claim and seven California state-law claims: (1) declaratory relief declaring AT&T's Wireless Customer Agreement unenforceable; (2) unlawful disclosure under the Federal Communications Act ("FCA"); (3) deceit by concealment; (4) misrepresentation; (5) negligence; (6) negligent supervision and training; (7) negligent hiring; and (8) breach of contract. He sought $24,000,000 in damages and up to $216,000,000 in punitive damages.

AT&T moved to dismiss Terpin's fraud claims and punitive damages claim. The district court granted the motion. It held that Terpin's deceit by concealment claim failed because he did not allege that AT&T had a duty to disclose, and his fraudulent misrepresentation claim failed because he did not allege that AT&T made a promise with no intent to perform. The district court also held that Terpin failed to allege facts sufficient to support punitive damages. It invited Terpin to seek leave to amend if he learned facts through discovery supporting punitive damages, but he never did so.

After the parties engaged in discovery, AT&T moved for summary judgment on Terpin's other claims. The district court granted the motion. First, the district court held that the economic loss rule barred Terpin's negligence claims because his claims were not "independent of" the Wireless

[1] Terpin also sued Pinsky and Pinsky's associate in separate lawsuits. He obtained a $22 million judgment against Pinsky and a $75 million judgment against Pinsky's associate. Pinsky's associate was also criminally prosecuted.

Customer Agreement. Second, the court held that Terpin's FCA claim failed because "[t]he undisputed facts establish that the SIM swap did not disclose any information that is protected under 47 U.S.C. § 222." Third, the court held that Terpin's breach of contract claim failed because he sought only consequential damages, which were unavailable to him under the parties' contract. Finally, the court held that AT&T was entitled to summary judgment on Terpin's declaratory judgment claim, both because the claim was moot and because Terpin failed to respond to AT&T's motion for summary judgment on that claim.

Terpin appealed both the dismissal order and the summary judgment order.

Standard of Review

We review the district court's order granting AT&T's motion to dismiss de novo. *In re Nektar Therapeutics Sec. Litig.*, 34 F.4th 828, 835 (9th Cir. 2022). We will affirm unless Terpin's allegations "contain sufficient factual matter, accepted as true, to state a claim to relief that is plausible on its face." *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009) (quoting *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 570 (2007)) (cleaned up); *see also* Fed. R. Civ. P. 8(a), 12(b)(6). On Terpin's two fraud claims, he must allege the fraud "with particularity" but may allege "[m]alice, intent, knowledge, and other conditions of a person's mind . . . generally." Fed. R. Civ. P. 9(b).

We also review the district court's order granting summary judgment for AT&T de novo. *Stevens v. Corelogic, Inc.*, 899 F.3d 666, 672 (9th Cir. 2018). Summary judgment is appropriate only if, viewing the facts and drawing all reasonable inferences in Terpin's favor, "there is no genuine dispute as to any material fact and [AT&T] is

entitled to judgment as a matter of law." Fed. R. Civ. P. 56(a); *see also Thomas v. Ponder*, 611 F.3d 1144, 1149–50 (9th Cir. 2010). That is, Terpin "need only show a triable issue of material fact to proceed to trial, not foreclose any possibility of the defendant's success on the claims." *See Sonner v. Schwabe N. Am., Inc.*, 911 F.3d 989, 992 (9th Cir. 2018) (citations omitted). "An issue of material fact is genuine 'if there is sufficient evidence for a reasonable jury to return a verdict for the non-moving party.'" *Thomas*, 611 F.3d at 1150 (quoting *Long v. County of Los Angeles,* 442 F.3d 1178, 1185 (9th Cir. 2006)).

Discussion

I. Terpin failed to plausibly allege fraud claims.

A. Deceit by concealment.

Terpin's first fraud claim rests on a "deceit by concealment" theory. He contends AT&T failed to disclose that the extra security it promised him "could readily be evaded or bypassed by AT&T employees acting in concert with individuals perpetrating SIM swap fraud."

A "deceit by concealment" claim requires, among other elements, that a defendant "concealed or suppressed a material fact" the defendant had "a duty to disclose" to the plaintiff. *Bank of Am. Corp. v. Superior Ct.*, 130 Cal. Rptr. 3d 504, 509–10 (Ct. App. 2011). A defendant has a duty to disclose when: (1) "the defendant is in a fiduciary relationship with the plaintiff"; (2) "the defendant had exclusive knowledge of material facts not known to the plaintiff"; (3) "the defendant actively conceals a material fact from the plaintiff"; or (4) "the defendant makes partial representations but also suppresses some material facts." *Deteresa v. Am. Broad. Cos., Inc.*, 121 F.3d 460, 467 (9th

Cir. 1997) (quoting *LiMandri v. Judkins*, 60 Cal. Rptr. 2d 539, 543 (Ct. App. 1997)). Terpin failed to plausibly allege that AT&T had a duty to disclose.

First, Terpin argues he sufficiently alleged that AT&T had "exclusive knowledge" of material facts not known to Terpin. We disagree. AT&T may have greater knowledge about its own "security practices," but it told Terpin its security measures have limits. It disclosed, for example, that "no security measures are perfect"; that AT&T "cannot guarantee" Terpin's personal information "will never be disclosed in a manner inconsistent with [the Privacy Policy]," such as disclosures stemming from "unauthorized acts by third parties that violate the law or [the Privacy Policy]"; and that AT&T "DOES NOT GUARANTEE SECURITY."[2] Given these disclosures, AT&T did not have "exclusive knowledge" that a bad actor could bypass the security measures AT&T provided Terpin.

Second, Terpin maintains that AT&T "actively concealed" that employees could bypass its security measures. But he failed to allege facts supporting an active concealment theory. Active concealment requires that the defendant take affirmative steps to prevent the plaintiff from discovering material facts. *See Rubenstein v. The Gap, Inc.*, 222 Cal. Rptr. 3d 397, 405 (Ct. App. 2017); *Lingsch v. Savage*, 29 Cal. Rptr. 201, 204 (Ct. App. 1963). Terpin alleges no facts suggesting that AT&T tried to prevent him from learning that an employee could circumvent AT&T's security measures. Terpin's allegations of "mere

[2] When reviewing an order granting a Fed. R. Civ. P. 12(b)(6) motion, we may consider documents attached to and referenced in the complaint. *See United States v. Ritchie*, 342 F.3d 903, 908 (9th Cir. 2003).

nondisclosure" are not enough to show active concealment. *Lingsch*, 29 Cal. Rptr. at 204.

Third, Terpin contends that AT&T made a misleading partial disclosure when it told him the six-digit code would give him heightened security. He argues that statement was misleading because AT&T did not disclose that a rogue employee could bypass the code. But AT&T's alleged partial disclosure in no way suggests that the heightened security would prevent all fraud. To the contrary, Terpin alleges that AT&T told him his account would be "much *less likely* to be subject to SIM swap fraud," and AT&T separately disclosed that it "cannot guarantee" its security measures will prevent a breach.

In short, Terpin failed to sufficiently allege that AT&T had a duty to disclose a material fact. We thus affirm the district court's dismissal of Terpin's deceit by concealment claim.

B. Fraudulent misrepresentation.

Terpin also asserts a fraud claim based on AT&T's affirmative misrepresentation. He alleges AT&T falsely promised it would give him "'extra security' in the form of a six-digit code to prevent future account takeovers," but a bad actor ultimately bypassed the code.

"A promise of future conduct is actionable as fraud only if made without a present intent to perform." *Magpali v. Farmers Grp., Inc.*, 55 Cal. Rptr. 2d 225, 231 (Ct. App. 1996). Terpin failed to sufficiently allege that AT&T made a promise with no intent to perform. Even if AT&T knew that the extra security measures it promised Terpin could be "readily bypassed or evaded," that does not support an inference that AT&T never intended to implement those

security measures. Making "a promise with an honest but unreasonable intent to perform is wholly different from making one with no intent to perform" and thus cannot be "false." *Tarmann v. State Farm Mut. Auto. Ins.*, 2 Cal. Rptr. 2d 861, 864 (Ct. App. 1991); *Magpali*, 55 Cal. Rptr. 2d at 232 ("[A]n erroneous belief, no matter how misguided, does not justify a finding of fraud.").

Beyond that, Terpin alleged that he discussed additional security measures "with AT&T representatives in Puerto Rico," but he did not describe who those representatives are or their authority to speak on AT&T's behalf. *Kearns v. Ford Motor Co.*, 567 F.3d 1120, 1124 (9th Cir. 2009) ("Averments of fraud must be accompanied by 'the who, what, when, where, and how' of the misconduct charged." (quoting *Vess v. Ciba-Geigy Corp. USA*, 317 F.3d 1097, 1106 (9th Cir. 2003))); *see also Tarmann*, 2 Cal. Rptr. 2d at 862–63 (explaining that a fraud claim against a corporation requires the plaintiff to specify "the names of the persons who made the allegedly fraudulent representations" and "their authority to speak").

Because Terpin failed to plausibly allege an affirmative misrepresentation, we affirm the district court's dismissal of his fraudulent misrepresentation claim.

II. Terpin failed to state a claim for punitive damages.

Terpin also seeks punitive damages. Punitive damages are available under California law if the plaintiff shows that the defendant engaged in "oppression, fraud, or malice." Cal. Civ. Code § 3294(a). And when the plaintiff seeks punitive damages against an entity, the plaintiff must show that "an officer, director, or managing agent" of the entity engaged in, authorized, or ratified the conduct giving rise to punitive damages. *Id.* § 3294(b). "Malice" is conduct intended "to

cause injury to the plaintiff" or "despicable conduct" carried out "with a willful and conscious disregard of the rights or safety of others." *Id.* § 3294(c)(1). "Oppression" is "despicable conduct that subjects a person to cruel and unjust hardship in conscious disregard of that person's rights." *Id.* § 3294(c)(2). Terpin did not allege sufficient facts to support punitive damages.

Terpin ties his punitive damages claims to two AT&T officers, Bill O'Hern and David Huntley. Terpin alleges that O'Hern and Huntley knew or should have known about AT&T's security flaws and the general risk of SIM swap fraud. But beyond a conclusory allegation that O'Hern and Huntley did "nothing to prevent" SIM swaps, Terpin alleges no facts plausibly suggesting that O'Hern and Huntley intended to harm Terpin or consciously disregarded a known risk to his AT&T account. Nor does Terpin allege that O'Hern or Huntley participated in or ratified AT&T's alleged fraudulent statements about the "extra security" on his account. And even though the district court told Terpin he could later seek leave to amend if he learned new facts supporting punitive damages, he never did so. Terpin thus failed to allege facts supporting an inference that AT&T's officers engaged in oppression, fraud, or malice. *See Alday v. Raytheon Co.*, 693 F.3d 772, 795 (9th Cir. 2012) (affirming judgment on the pleadings on punitive damages claim because the plaintiffs "alleged no facts showing that the defendants' conduct" was "sufficiently outrageous or egregious to warrant an award of punitive damages against them" (cleaned up)).[3]

[3] The district court did not, as Terpin contends, apply a "heightened pleading standard" to Terpin's punitive damages allegations. The district

We affirm the district court's dismissal of Terpin's punitive damages claim.

III. Terpin's breach of contract claim is unavailable.

Terpin also asserts a breach of contract claim. He alleges that AT&T breached several of its obligations under the Privacy Policy, which is incorporated in the Wireless Customer Agreement. Terpin seeks only consequential damages on his contract claim: the loss of his cryptocurrency to hackers. *Lewis Jorge Constr. Mgmt., Inc. v. Pomona Unified Sch. Dist.*, 102 P.3d 257, 261 (Cal. 2004) (explaining that general damages are "those that flow directly and necessarily from a breach of contract," while consequential damages "are those losses that do not arise directly and inevitably" from a breach but "are secondary or derivative losses arising from circumstances that are particular to the contract or to the parties").

Consequential damages, however, are unavailable to Terpin. The Wireless Customer Agreement bars recovery "for any indirect, special, punitive, incidental or consequential losses or damages" Terpin "may suffer by use of, or inability to use, Services, Software, or Devices provided by or through AT&T." Limitation of liability clauses like this one "have long been recognized as valid in California." *Food Safety Net Servs. v. Eco Safe Sys. USA, Inc.*, 147 Cal. Rptr. 3d 634, 641–42 (Ct. App. 2012) (quoting *Markborough Cal., Inc. v. Superior Ct.*, 277 Cal. Rptr. 919, 925 (Ct. App. 1991)). Because Terpin seeks only consequential damages, his breach of contract claim is barred by the parties' limitation of liability clause.

---

court applied Rule 8 federal pleading standards and held that Terpin failed to meet those standards.

Terpin mentioned in a footnote in his opening brief that the district court "ignored" his allegations that the Wireless Customer Agreement is "a contract of adhesion" and the limitation of liability clause "is unconscionable because it violates public policy." But "adhesion" contracts are not per se unconscionable under California law, *Poublon v. C.H. Robinson Co.*, 846 F.3d 1251, 1260–61 (9th Cir. 2017), and Terpin offers no other argument in his opening or reply brief explaining why the agreement is unconscionable. He thus forfeited this argument. *E.g.*, *Indep. Towers of Wash. v. Washington*, 350 F.3d 925, 929 (9th Cir. 2003) (an appellant forfeits issues not "specifically and distinctly" argued in the opening brief).

Terpin also argues that his contract claim rests not just on the Privacy Policy, but also on AT&T's "separate" oral agreement to provide "extra security." Terpin did not allege this contractual theory in his complaint, and the district court did not err by declining to consider this new theory Terpin raised for the first time in response to a motion for summary judgment. *See Pickern v. Pier 1 Imports (U.S.), Inc.*, 457 F.3d 963, 968–69 (9th Cir. 2006) (holding that a plaintiff could not raise new allegations supporting her claim for the first time at summary judgment); *Wasco Prods., Inc. v. Southwall Techs., Inc.*, 435 F.3d 989, 992 (9th Cir. 2006) ("Simply put, summary judgment is not a procedural second chance to flesh out inadequate pleadings." (quoting *Fleming v. Lind-Waldock & Co.*, 922 F.2d 20, 24 (1st Cir. 1990))). But even if Terpin had alleged a contractual promise to add extra security, he does not argue that the oral agreement somehow superseded or extinguished the written agreement. In fact, an oral modification of the agreement would "not wholly extinguish" the rest of the agreement; it would leave "the remaining portions" unaffected by the modification

"intact." *Davies Mach. Co. v. Pine Mountain Club, Inc.*, 113 Cal. Rptr. 784 (Ct. App. 1974) (quoting *Eluschuk v. Chem. Eng'rs Termite Control, Inc.*, 54 Cal. Rptr. 711, 715 (Ct. App. 1966)); *see also Howard v. County of Amador*, 269 Cal. Rptr. 807, 817 (Ct. App. 1990).

At bottom, Terpin's breach of contract claim for consequential damages is barred by the parties' agreement. We thus affirm the district court's summary judgment in AT&T's favor on Terpin's contract claim.[4]

IV. Terpin's negligence claims are barred by the economic loss rule.

The district court held that the economic loss rule bars Terpin's negligence claims. That rule "functions to bar claims in negligence for pure economic losses in deference to a contract between litigating parties." *Sheen v. Wells Fargo Bank, N.A.*, 505 P.3d 625, 632 (Cal. 2022). In other words, the rule "prevents the law of contract and the law of tort from dissolving one into the other." *Robinson Helicopter Co., Inc. v. Dana Corp.*, 102 P.3d 268, 272–73 (Cal. 2004) (cleaned up). Thus, "claims for monetary losses between contractual parties are barred by the economic loss rule . . . when they arise from — or are not independent of — the parties' underlying contracts." *Sheen*, 505 P.3d at 633.

[4] The district court also granted summary judgment on Terpin's claim for declaratory relief alleging that the parties' agreement was unenforceable. On appeal, Terpin argues only that his declaratory judgment claim will no longer be moot if the court reverses the district court's ruling on his other claims. But he does not address the district court's holding that summary judgment was appropriate because Terpin did "not respond to AT&T's Motion on the claim for declaratory relief." Because Terpin does not challenge that ruling on appeal, we affirm.

The economic loss rule serves several purposes. Among other things, it "protects the bargain the parties have made against disruption by a tort suit" and "allows parties to make dependable allocations of financial risk without fear that tort law will be used to undo them later." *Sheen*, 505 P.3d at 625 (quoting Restatement (Third) of Torts, Liab. for Econ. Harm § 3 cmt. b (Am. L. Inst. 2020)). And when "[v]iewed in the long run," the rule "prevents the erosion of contract doctrines by the use of tort law to work around them." *Id.*

The California Court of Appeal recently applied the economic loss rule in *Moore v. Centrelake Medical Group, Inc.*, 299 Cal. Rptr. 3d 544, 561–63 (Ct. App. 2022). There, the plaintiffs had contracts with a health care provider "establishing their provider-patient relationships." *Id.* at 561. The agreements included a privacy policy requiring that the provider "maintain adequate data security practices to protect appellants' [personal information] from unauthorized access by third parties." *Id.* at 548. After hackers obtained the plaintiffs' personal information in a data breach, the plaintiffs sued for breach of contract, negligence, and other claims. *Id.* The court held that the economic loss rule barred the plaintiffs' negligence claim because they "failed to show their claim is independent of their contracts with" the provider. *Id.* at 561. In fact, the plaintiffs gave the provider their personal information "pursuant to the contracts," and the plaintiffs' "asserted injuries arose from [the provider]'s failure to provide data security allegedly promised in their contracts." *Id.*

So too here. Terpin's negligence claims rest on AT&T's alleged duty to adequately protect Terpin's account

information.[5] But he fails to identify a duty "independent of" the contract. To the contrary, Terpin describes AT&T's "duties" as aligned with "commitments" AT&T made in the Privacy Policy to "protect [customers'] information," "keep [a customer's] information safe," ensure that AT&T employees follow "legal requirements and company policies surrounding the . . . security and privacy of [customers'] records," and "[l]imit[] access" to customer information. Those "commitments" are incorporated in the Wireless Customer Agreement, and they are the basis for Terpin's breach of contract claim. What's more, Terpin's negligence claims seek to impose duties that would exceed express limitations in the parties' agreement, including a bar on recovery for any indirect or consequential losses, and disclaimers making clear that AT&T's security measures are not impenetrable. "To impose a tort duty in such circumstances would go further than creating obligations unnegotiated or agreed to by the parties; it would dictate terms that are *contrary* to the parties' allocation of rights and responsibilities." *Sheen*, 505 P.3d at 634.

Terpin posit that Section 222 of the FCA creates an independent duty. We decline to hold that Section 222 imposes a duty of care giving rise to a state-law negligence claim. To be sure, a duty of care "'may arise through statute' or by operation of the common law." *Sheen*, 505 P.3d at 630. And the FCA says that wireless carriers have "a duty to protect the confidentiality of proprietary information of . . . customers." 47 U.S.C. § 222(a). But Terpin has not cited—

[5] On appeal, Terpin does not distinguish his different negligence claims and refers generally to AT&T's "duty" to "protect its customers' communications." We thus discuss Terpin's negligence claims together and address AT&T's duty as Terpin frames it.

nor have we found—any authority suggesting that this federal *statutory* duty creates a duty of care for a negligence claim under California law. *Moore* illustrates this point. In *Moore*, the plaintiffs relied on federal HIPAA regulations as the source of the alleged duty underlying their negligence claims. *Moore*, 299 Cal. Rptr. 3d at 561. Much like the FCA's requirement that wireless carriers protect customer information, HIPAA imposes statutory duties on health care providers to protect patients' "protected health information." 45 C.F.R. § 164.530(c)(1); *Moore*, 299 Cal. Rptr. 3d at 561. But the only cases the *Moore* plaintiffs could point to "did not address an independent duty of care under any statute (much less HIPAA), instead addressing the evidentiary doctrine of negligence per se, which concerns *standards* of care." *Moore*, 299 Cal. Rptr. 3d at 561; *see also Tucker v. CBS Radio Stations, Inc.*, 124 Cal. Rptr. 3d 245, 254 (Ct. App. 2011) (noting that the plaintiffs argued certain federal regulations imposed a duty, but they did "not cite any case holding that these regulations independently establish a *negligence duty of care*" (emphasis added)). Likewise here, we know of no authority ever suggesting that Section 222 creates a duty of care enforceable through a negligence claim. Indeed, allowing a plaintiff to rely on a federal statutory requirement like Section 222 to create a state-law negligence duty to protect customer information would significantly expand California tort law. *Cf. Sheen*, 505 P.3d at 648 (explaining that the "ill defined and amorphous" nature of tort liability and the "vagueness and breadth of plaintiff's proposed duty" counseled "against imposing that duty"). We decline to open that door.

In all events, even if the FCA creates a duty of care enforceable through a state-law negligence claim, Terpin still fails to show that this duty is "independent of" the

parties' contract. A contracting party cannot evade the economic loss rule by asserting a negligence claim based on a statutory duty instead of a common-law one. Whatever the source of the duty of care (common law or statute), the economic loss rule bars negligence claims for pure monetary losses that "arise from — or are not independent of — the parties' underlying contracts." *Sheen*, 505 P.3d at 633. Again, AT&T had access to Terpin's customer information through its contractual relationship with him. And Terpin's claimed tort injuries stem from AT&T's "failure to provide" security over his information "allegedly promised in their contract[]." *Moore*, 299 Cal. Rptr. 3d at 561. That is precisely what the economic loss rule prohibits.

Terpin alternatively contends that the economic loss rule does not apply to "contracts of adhesion." We disagree. As Terpin accurately notes, one rationale for the economic loss rule is "protect[ing] the bargain the parties have made against disruption by a tort suit," *Sheen*, 505 P.3d at 633 (quoting Restatement § 3 cmt. b), and a contract of adhesion does not involve a negotiated bargain. But the economic loss rule serves many purposes regardless of the type of agreement, including allowing parties to allocate risks before entering contracts, reducing confusion stemming from lawsuits with redundant contract and tort theories, and preventing "the erosion of contract doctrines by the use of tort law to work around them." Restatement § 3 cmt. b. Indeed, in *Sheen*, there was a similar imbalanced bargaining power between the plaintiff (an individual borrower) and the defendant (Wells Fargo), but the Supreme Court of California still held that the economic loss rule barred the plaintiff's negligence claim. 505 P.3d at 633.

To be clear, we hold only that the economic loss rule bars Terpin's *negligence* claims. This holding does not, as Terpin

suggests, let AT&T "absolve itself" of its "statutory duty" under the FCA. Section 222 of the FCA still creates a statutory duty enforceable through a private right of action. *See* 47 U.S.C. § 206. Terpin can and did assert that statutory claim (as we discuss below), and the economic loss rule does not bar it. *See Sheen*, 505 P.3d at 646–47 (rejecting the plaintiff's argument that he was left "without any remedy at all," because he could have asserted other causes of action besides the general negligence claim barred by the economic loss rule).

V. Terpin established a triable issue over whether the fraudulent SIM swap gave hackers access to information protected under the FCA.

Finally, we turn to Section 222 of the FCA. *See* 47 U.S.C. § 206. Section 222 was enacted to protect customer privacy against the backdrop of the Act's broader goal of fostering competition in the telecommunications industry. *See U.S. W., Inc. v. FCC*, 182 F.3d 1224, 1236 (10th Cir. 1999) ("While the broad purpose of the [FCA] is to foster increased competition in the telecommunications industry, . . . the specific and dominant purpose of § 222 is the protection of customer privacy." (citing S. Rep. No. 104-230, at 205 (1996) (Conf. Rep.))).

Section 222(a) provides that telecommunications carriers have "a duty to protect the confidentiality of proprietary information of, and relating to, other telecommunication carriers, equipment manufacturers, and customers." 47 U.S.C. § 222(a). Section 222(c) prohibits carriers from using, disclosing, or permitting access to "customer proprietary network information" ("CPNI") with few exceptions. 47 U.S.C. § 222(c)(1), (d); 47 U.S.C. § 222(h)(1) (defining CPNI). Congress also gave

the FCC rulemaking and enforcement authority, *see* 47 C.F.R. § 0.311, and the FCC has adopted rules implementing Section 222, 47 C.F.R. § 64.2001 *et seq*.

The parties dispute the scope of Section 222. Terpin contends that the statute protects both CPNI and a broader category of customer "proprietary information." He argues that subsection (a) uses different language than subsection (c), and "the use of different words or terms" in the same statute generally means "that Congress intended to convey a different meaning for those words." *S.E.C. v. McCarthy*, 322 F.3d 650, 656 (9th Cir. 2003). AT&T maintains that Section 222 protects only CPNI, not a broader category of customers' "proprietary information." AT&T argues that subsection (a) (titled "In general") simply sets out the general obligations in Section 222, and the remaining subsections "flesh out the precise contours of that obligation." According to AT&T, if subsection (a) imposes a broad obligation to protect customers' "proprietary information," then much of the more specific provisions in Section 222 governing CPNI would be "swallowed by the general" duty and rendered mere "superfluity." *RadLAX Gateway Hotel, LLC v. Amalgamated Bank*, 566 U.S. 639, 645 (2012). We need not decide which of these proposed interpretations is correct. Even under AT&T's narrower construction of Section 222, there is a triable issue over whether AT&T "permit[ted] access" to Terpin's CPNI. 47 U.S.C. § 222(c)(1); *see Rust v. Johnson*, 597 F.2d 174, 181 (9th Cir. 1979) (declining to reach issues "unnecessary to our decision" (citing *Immigr. & Naturalization Serv. v. Bagamasbad*, 429 U.S. 24, 25 (1976))).

CPNI is "information that relates to the quantity, technical configuration, type, destination, location, and amount of use of a telecommunications service" that a

customer makes "available to the carrier . . . solely by virtue of the carrier-customer relationship." 47 U.S.C. § 222(h)(1)(A). This includes, for example, information such as incoming or outgoing communications on a customer's account; the time, location, frequency, or length of communications on a customer's account; billing or costs charged to a customer's account; and any service features associated with a customer's account. *See* 47 U.S.C. § 222(h)(1); *see also Nat'l Cable & Telecomms. Ass'n v. FCC*, 555 F.3d 996, 997 (D.C. Cir. 2009); *In the Matter of Implementation of the Telecomms. Act of 1996: Telecomms. Carriers Use of Customer Proprietary Network Info. & Other Customer Info. Ip-Enabled Servs.*, 22 F.C.C. Rcd. 6927, 6931 (2007) ("2007 FCC CPNI Order"). Here, there is a genuine issue of material fact over whether AT&T gave hackers access to Terpin's CPNI. Terpin produced evidence that the SIM swap allowed Pinsky to associate Terpin's customer account with a new mobile device in Pinsky's control and gave Pinsky access to all future communications with Terpin's phone number. A jury could thus find that AT&T gave hackers access to Terpin's CPNI in two ways.

First, the SIM swap gave Pinsky "access" to "information that relates to . . . the technical configuration" of Terpin's telecommunications service. 47 U.S.C. § 222(h)(1)(A). The technical "configuration" of a customer's telecommunications service includes the devices associated with that service. *Configuration*, Merriam-Webster, https://www.merriam-webster.com/dictionary/configuration (last visited August 1, 2024) (the "parts," "elements," or "components" that make up something); *see also Configuration*, Cambridge Dictionary, https://dictionary.cambridge.org/us/dictionary/english/configuration (last visited August 1, 2024) ("the way in which

something, such as a computer system or software, is organized to operate"). Terpin pointed to evidence that a "SIM enables a mobile device to be associated with a specific phone number" to "route communications" and "associat[e] the service with a customer account." He also pointed to Pinsky's deposition testimony explaining how Pinsky successfully updated Terpin's AT&T account to associate it with a new device: he told Smith "that [he had] a phone number at AT&T that [he] need[ed] to be SIM swapped" and asked Smith "to port Mr. Terpin's phone number onto another SIM card" in Pinsky's control. The notes on Terpin's account also confirmed that Terpin's account was updated to replace a prior SIM with a new SIM "per customer request."

The district court focused on whether any CPNI was "disclosed" to Pinsky during the SIM swap. But Section 222(b)(1) does not merely prohibit the use or disclosure of CPNI, it also prohibits "permit[ting] *access* to" CPNI. 47 U.S.C. § 222(c)(1) (emphasis added). The FCC's rules implementing Section 222 likewise require that carriers "take reasonable measures to discover and protect against attempts to gain unauthorized *access* to CPNI." 47 C.F.R. § 64.2010(a) (emphasis added). Permitting "access" to information is broader than disclosing it: access includes an "opportunity" or "ability to" obtain or use the information. *Access*, Black's Law Dictionary (11th ed. 2019); *Access*, Merriam-Webster, https://www.merriam-webster.com/dictionary/access (last visited August 1, 2024) ("freedom or ability to obtain or make use of something"). Through the SIM swap, Pinsky updated Terpin's wireless account to associate Terpin's phone number with a new SIM in Pinsky's control. A jury could thus find that he necessarily gained "access" to the technical configuration of Terpin's

account. Even if the evidence at this stage does not "foreclose any possibility" of AT&T's success on Terpin's claim, it is sufficient to "show a triable issue of material fact." *Sonner*, 911 F.3d at 992.

Second, the SIM swap gave Pinsky access to information "that relates to" the "type, destination, location, and amount of use of a telecommunications service" by allowing Pinsky to receive all incoming communications sent to Terpin's phone number. 47 U.S.C. § 222(h)(1)(a). The district court held that the SIM swap disclosed only Terpin's phone number, which is not CPNI. But that is an overly simplistic view of a SIM swap. A SIM swap does not merely disclose a phone number—it gives a person *control* over the phone number and access to any future communications involving that phone number. Terpin pointed to Pinsky's deposition testimony explaining that, after the SIM swap, he requested password reset messages on Terpin's Gmail and Microsoft accounts and received those messages on the device he associated with Terpin's AT&T account. Pinsky also testified that he could login to Terpin's Microsoft account because he had "control over Mr. Terpin's phone account by virtue of the . . . SIM swap." The password reset messages themselves are communications sent to Terpin's phone number and thus qualify as CPNI. *See* 47 U.S.C. § 222(h)(1); 2007 FCC CPNI Order.

AT&T contends that "the only communications Terpin identifies are messages *Pinsky* requested and received [while] resetting various online passwords." Thus, AT&T argues, because "Terpin didn't generate or request any of those messages," there was "no customer information for § 222 to protect." AT&T's counsel likewise maintained during oral argument that, once a SIM swap occurs, no information generated on a customer's account belongs to

the customer. Not so. Even if Pinsky fraudulently requested the password reset messages from Terpin's accounts, the messages were intended for *Terpin* and sent to *Terpin*'s phone number. A hacker's fraudulent use of a customer's account does not transform the customer's account into the *hacker's* account. Consider a bad actor who poses as a bank customer and opens a new credit card under the customer's name. If the customer later tried to cancel the credit card, would the bank say the credit card did not belong to the customer because the bad actor—not the customer—opened the card? Surely not. Nor does the identity of the person requesting information change the nature of the information. Even though Pinsky requested the password reset messages, the messages were sent to Terpin's AT&T phone number and thus were made available to AT&T "solely by virtue of the carrier-customer relationship." 47 U.S.C. § 222(h)(1)(a).

Adopting AT&T's constrained view of CPNI would lead to absurd results. If Pinsky had walked into the AT&T affiliate store, asked Smith to print Terpin's recent call log, and looked at the call log, AT&T would not dispute that Pinsky had access to CPNI. Yet under AT&T's view, Pinsky had no access to CPNI when he walked into the store, updated Terpin's account to change the SIM associated with Terpin's phone number, gained control over all incoming communications with Terpin's phone number, and received confidential password reset messages sent to Terpin's phone number. Our decision avoids this paradox.[6]

[6] Our decision is also consistent with the FCC's views. In a report addressing new proposed CPNI rules, the FCC recognized that SIM swap fraud "allows the bad actor to gain access to information associated with the customer's account, including CPNI, and gives the bad actor control

In sum, Terpin presented a triable issue over whether AT&T gave hackers "access" to Terpin's CPNI through the SIM swap. We thus reverse the district court's holding that "the SIM swap did not disclose any information that is protected under 47 U.S.C. § 222."

VI. The district court should consider AT&T's proximate cause arguments on remand.

AT&T alternatively argues this court can affirm the summary judgment in its favor based on a lack of proximate cause. The district court did not reach this issue. While we may affirm "on any ground supported by the record," whether proximate cause existed for each claim is "not purely legal" and would require that we "determine whether the evidence creates a genuine issue of material fact." *MacIntyre v. Carroll Coll.*, 48 F.4th 950, 956 (9th Cir. 2022) (quoting *U.S. ex rel. Ali v. Daniel, Mann, Johnson & Mendenhall*, 355 F.3d 1140, 1144 (9th Cir. 2004)); *see also Ileto v. Glock Inc.*, 349 F.3d 1191, 1206 (9th Cir. 2003) (explaining that proximate cause is "generally a question of fact" unless the facts are undisputed and only one inference can "reasonably be drawn from those facts" (quoting *Garman v. Magic Chef, Inc.*, 173 Cal. Rptr. 20, 22 (Ct. App. 1981))). We thus remand to the district court to consider this issue "in the first instance." *MacIntyre*, 48 F.4th at 956.

Conclusion

We affirm in part and reverse in part. Terpin's fraud claims fail because he failed to allege sufficient facts to

---

of the customer's phone number so that the bad actor receives the text messages and phone calls intended for the victim." *In the Matter of Protecting Consumers from Sim Swap & Port-Out Fraud*, No. FCC23-95, 2023 WL 9291563, at *2 (OHMSV Nov. 16, 2023).

establish that AT&T had a duty to disclose a material fact or that AT&T made any actionable misrepresentations. Terpin also failed to plausibly allege conduct giving rise to punitive damages. Terpin's breach of contract claim fails because the limitation of liability clause in the Wireless Customer Agreement precludes the damages he seeks. And Terpin's negligence claim is barred under the economic loss doctrine. But Terpin presented a triable issue on his claim under Section 222 of the FCA. He pointed to evidence that the SIM swap gave hackers "access" to his CPNI in violation of Section 222. We thus reverse the district court's grant of summary judgment on that claim.

AFFIRMED in part, **REVERSED** in part, and **REMANDED**. Each party shall bear its own costs on appeal.