No. 24-2643

UNITED STATES COURT OF APPEALS FOR THE NINTH CIRCUIT

X CORP.,

Plaintiff-Appellant,

v.

CENTER FOR COUNTERING DIGITAL HATE, INC.;
CENTER FOR COUNTERING DIGITAL HATE LTD.;
STICHTING EUROPEAN CLIMATE FOUNDATION,

Defendants-Appellees.

Appeal from the United States District Court
for the Northern District of California
Civil Case No. 3:23-cv-03836
(Honorable Charles R. Breyer)

OPENING BRIEF OF PLAINTIFF-APPELLANT

July 5, 2024 James Jonathan Hawk MCDERMOTT WILL & EMERY 2049 Century Park East Suite 3200 Los Angeles, CA 90067 (310) 788-4181 jhawk@mwe.com	Charles J. Cooper David H. Thompson Peter A. Patterson John D. Ohlendorf Samuel D. Adkisson Athanasia O. Livas COOPER & KIRK, PLLC 1523 New Hampshire Ave., N.W. Washington, DC 20036 (202) 220-9600 ccooper@cooperkirk.com
Attorneys for Plaintiff-Appellant X Corp.	

CORPORATE DISCLOSURE STATEMENT

Pursuant to Federal Rule of Appellate Procedure 26.1(a), X Corp. submits this corporate disclosure statement. X Corp. is a privately held corporation. Its parent corporation is X Holdings Corp. No publicly traded corporation owns 10% or more of the stock of X Corp. or X Holdings Corp.

TABLE OF CONTENTS

Page

TABLE OF AUTHORITIES

Cases **Page**

Rules & Codes

Other Authorities

INTRODUCTION

This is a case about data security and the contractual terms that protect it. It arises from two entities' unlawful access to private data belonging to X Corp. ("X"), the social media platform formerly known as Twitter. Beginning in 2021, two European activist organizations—the Center for Countering Digital Hate ("CCDH") and the Stichting European Climate Foundation ("ECF")—conspired to give CCDH unauthorized and unlawful access to X's private data, including data held by X's third-party corporate partner, Brandwatch, on secure servers in the United States. CCDH then used and manipulated this data to produce a report calling for advertisers to boycott X. Because CCDH obtained X's data by breaching its own contract with X and by inducing the breach of X's contract with Brandwatch, X brought this suit, seeking to recover the tens of millions of dollars of lost advertising revenue it had suffered as a result.

Not content to adjudicate the ordinary contract and tort claims actually brought by X, the district court first transformed the lawsuit into a First Amendment case and then dismissed it for failing to meet the constitutional standards governing a defamation claim—a claim that *X did not bring*. Although X's suit concerns Defendants' unlawful *access* to its data—not the content of the reports CCDH used that data to publish—the district court divined that X's true "purpose" in bringing its suit was "punishing the Defendants for their speech," 1-ER-34, and so it struck

X's claims under California's statutory regime governing "Strategic Lawsuits Against Public Participation" ("anti-SLAPP"). Its reasoning in doing so is flawed in multiple independent ways, and this Court should reverse.

First, the district court's First Amendment framing rewrites the complaint actually before it. X has not asserted a defamation claim and, instead, challenges Defendants' unprotected, non-expressive *conduct*: the wrongful access to and use of X's data. But under the district court's theory, because X *could* have pleaded a defamation claim, any other well-pleaded claims must be dismissed, given that non-defamation claims of course do not meet the elements of defamation. This novel framework ignores the complaint X actually wrote, finds no basis in any binding precedent, and is in fact foreclosed by binding precedent from this Court and the Supreme Court. X seeks ordinary contract damages—not reputation damages that would be available in a defamation case—and the fact that it *chose not* to bring a defamation claim seeking compensation for the harm to its reputation does not mean that the First Amendment limits its ability to recover the ordinary, foreseeable losses caused by Defendant's breach. And the district court's invocation of the First Amendment to dismiss X's tort claims fails for similar reasons.

The district court's flawed reasoning in dismissing X's claims under the Computer Fraud and Abuse Act ("CFAA") are equally unpersuasive. There can be no serious doubt that X's allegations make out a violation of that Act. CCDH

fraudulently accessed a protected computer—Brandwatch's servers—and then used valuable data stored there, belonging to X, without paying for it. The district court thought that the damages X suffered as a result—tens of thousands of dollars spent investigating, assessing, and responding to the breach—were not compensable under the CFAA. But that conclusion, based on stray dicta from two decisions that did not concern the CFAA's loss provision, is contrary to the binding precedent of this Court and decisions of every Circuit to have actually addressed the issue.

The district court made other errors as well. It dismissed ECF as beyond its jurisdiction, even though the tortious act that gave rise to X's claims against ECF—the unauthorized transmittal of its login credentials to CCDH—*occurred in the United States*. That fact vests American courts with personal jurisdiction under the settled principle that a forum may exercise jurisdiction over a foreign defendant who commits a tortious act *in the forum* against *a resident of the forum*. And even setting that rule aside, ECF's tortious conduct was purposefully directed at the United States by any measure. Finally, not content with amending X's complaint for it and then dismissing it for failing to state a claim X did not bring, the court proceeded to *deny X leave to amend its own complaint.* The district court provided no legitimate reason that amendment would be futile or dilatory, and provided no explanation at all for why it denied amendment of the claims regarding ECF.

For any of these independent reasons, this Court should reverse.

JURISDICTION

The district court had jurisdiction under 28 U.S.C. § 1332(a) and 28 U.S.C. §§ 1331, 1367(a). The district court entered final judgment on March 25, 2024. 1-ER-3. X timely noticed its appeal on April 23, 2024. 1-ER-142–43. This Court has jurisdiction under 28 U.S.C. § 1291.

STATEMENT OF THE ISSUES

I. Whether X's state-law claims arising out of CCDH's unauthorized access to and use of data are subject to California's anti-SLAPP statute.

II. Whether X plausibly alleged that CCDH breached its contract with X by scraping the X platform without authorization.

III. Whether X plausibly alleged violations of the Computer Fraud and Abuse Act.

IV. Whether X plausibly alleged that CCDH and ECF either interfered with or induced Brandwatch to breach its contract with X.

V. Whether ECF is subject to personal jurisdiction in the United States.

VI. Whether the district court erred in denying X leave to amend.

STATUTORY ADDENDUM STATEMENT

Pertinent constitutional provisions and statutes are set forth in the statutory addendum. *See infra* Add.1–Add.3.

STATEMENT OF THE CASE

I. Factual Background

X provides a free online platform allowing users to express their viewpoints and share information on the internet. To set basic ground-rules and protect the security of its platform, X has a contract, its Terms of Service, to which all users agree when they register to use the platform. 1-ER-102. X's Terms of Service explicitly prohibit the practice of "scraping," a data aggregation and manipulation practice that involves extracting massive amounts of data from a website through automated means. 1-ER-37. As the district court recognized, scraping "can be harmful not only to the users of a website but also to the website itself." 1-ER-73. Scraping "is bad for [the platform] and its members: [it] burdens [the platform's] servers, inhibiting the site's performances . . . [and] scrapers may retain and sell members' deleted information, interfering with members' control over or expectations regarding their information." *hiQ Labs, Inc. v. LinkedIn Corp.*, 639 F. Supp. 3d 944, 954 (N.D. Cal. 2022). "Accumulated scraped data is also vulnerable to security breaches." Geoffrey Xiao, *Bad Bots: Regulating the Scraping of Public Personal Information*, 34 HARV. J.L. & TECH. 701, 708 (2021). Thus, "users trust

websites to enforce the[ir] terms of service and to protect users from scraping." *Id.* at 710.

X's claims center around the conduct of three parties: Brandwatch, a company that provides brand monitoring tools and is not a party to this case, and defendants CCDH and ECF. CCDH is an activist organization dedicated to "stop[ping] the spread" of what it deems to be "online hate and disinformation," primarily through advocating for social media censorship by calling for advertising boycotts. Home Page, CCDH, https://bit.ly/4bt0ZAv (last visited July 3, 2024).[1] Beginning at least in March 2021, CCDH coordinated with ECF, a foreign activist organization, to obtain private X data for the purpose of producing public reports calling for an advertising boycott of X. 1-ER-105.

CCDH and ECF obtained X's secure, private data through two unlawful means. First, CCDH and ECF coordinated to unlawfully access private data that was owned by X but stored by Brandwatch. X partners with Brandwatch to provide enterprise brand monitoring tools to its customers. 1-ER-106–07. Brandwatch's agreements with X give Brandwatch access to certain private data, which Brandwatch's customers can access via secure login credentials. *Id.* Only users with login credentials provided by X and/or Brandwatch can access this data, which is

[1] CCDH has a legal entity in the United Kingdom, CCDH UK, and the United States, CCDH US. Unless context requires otherwise, we refer to both entities as "CCDH."

located on secure servers in the United States. *Id.* Brandwatch's agreements with X forbid Brandwatch from transferring or providing access to the Licensed Materials to third parties. *Id.* ECF is a customer of Brandwatch and has login credentials to access X's data. *Id.*

CCDH induced and conspired with ECF to provide CCDH with ECF's login credentials to access X's private data. 1-ER-106. ECF "on several occasions" transmitted its Brandwatch login credentials to CCDH's United States subsidiary, CCDH US, which is headquartered in and operates from the United States. 1-ER-105, CCDH engaged in these acts intentionally and with the intent to harm X. 1-ER-111.

Second, CCDH also obtained some of the data used in its reports by scraping X's platform. CCDH is a registered user of X and, as part of registering to use the platform, voluntarily agreed that "scraping the Services without the prior consent of [X Corp.] is expressly prohibited." 1-ER-109. Despite this, CCDH openly admitted that, "[t]o gather tweets from each of the ten reinstated accounts, [CCDH's] researchers used the social media web-scraping tool SNScrape." *Id.* "CCDH engaged in its unlawful scraping with the intent to improperly obtain data that would be used to cause X Corp. to lose significant advertising revenues." 1-ER-113.

As a result of its scraping and improper access to X's data, CCDH created several "reports" publicly manipulating and cherry-picking from the X data. 1-ER-

107. One such "report," entitled "Toxic Twitter," explicitly called for companies to stop advertising on X. 1-ER-108. As a direct and proximate result, at least eight organizations immediately paused advertising spending on X. 1-ER-134. Others halted plans for future advertising, pointing to CCDH's November 10, 2022 "report" as a barrier to reactivating campaigns. 1-ER-134–35. This lost advertising has cost X tens of millions of dollars. 1-ER-135. Further, X has spent considerable resources investigating and remediating CCDH's breach of contract and ECF and CCDH's infiltration of X's data security. 1-ER-104.

II. Procedural Background

X brought suit against CCDH and ECF, raising four claims: (1) breach of contract against CCDH; (2) violation of the CFAA in connection with CCDH's improper access to the Brandwatch data against all Defendants; (3) intentional interference with contractual relations, and (4) inducing breach of contract as to Brandwatch's agreement with X, both against all Defendants. 1-ER-135–40. In addition to CCDH and ECF, X also named Doe Defendants to be named after discovery reveals their identities.

Defendants moved to dismiss under FED. R. CIV. P. 12(b)(6) and to strike under California's anti-SLAPP statute, which permits a "special motion to strike" for causes of action based on acts furthering First Amendment rights unless the plaintiff establishes some probability of prevailing. 1-ER-43. On March 25, 2024,

the district court granted CCDH's motions to strike and dismiss the California state-law claims, 1-ER-84–85, and granted the Defendants' motions to dismiss the federal law claims under 12(b)(6). 1-ER-85. Additionally, the district court held that it lacked personal jurisdiction over ECF and dismissed the Doe Defendants. 1-ER-33. The district court denied X leave to amend. X appealed.

STANDARD OF REVIEW

This Court "review[s] de novo the grant or denial of an anti-SLAPP motion," and "exercise[s] independent judgment in determining whether … the challenged claims arise from protected activity." *Park v. Bd. of Trs. of Cal. State Univ.*, 393 P.3d 905, 911 (Cal. 2017). The Court does not "weigh the evidence," rather, it must "accept plaintiff's submissions as true and consider only whether any contrary evidence from the defendant establishes its entitlement to prevail as a matter of law." *Id.*

Under Federal Rule of Civil Procedure 12(b)(6), the Court must "accept factual allegations in the complaint as true and construe the pleadings in the light most favorable" to X, the non-moving party. *Manzarek v. St. Paul Fire & Marine Ins. Co.*, 519 F.3d 1025, 1031 (9th Cir. 2008).

SUMMARY OF ARGUMENT

The district court erred in dismissing X's Amended Complaint in several independent ways.

I. First, the court erred in applying California's anti-SLAPP statute to X's claims, which arise from the defendants' non-expressive conduct, not protected speech.

II. Second, the district court erred in striking X's breach of contract claims. X plausibly alleged each element of those state-law claims, and the district court concluded otherwise only by grafting First Amendment principles from the *defamation* context onto ordinary breach of contract claims that are not based on protected speech. The court also erroneously held that X had not met the standard for "special damages" even though X has plausibly shown that CCDH would have contemplated that its wrongful scraping of X data for the purpose of deterring advertisers would in fact result in the desired effect.

III. Third, the district court erred in dismissing X's tort claims against CCDH and ECF for interfering with X's contract with Brandwatch. The court held that the causal link between Defendants' scheme and CCDH's unlawful access to Brandwatch's data in violation of its contract with X was too attenuated, but in reality it is difficult to imagine a tighter causal chain: CCDH's deceptive and unauthorized access *necessarily caused* Brandwatch to breach its agreement to keep

X's data secure and private from third parties. And the court's conclusion that X had not adequately alleged damages flowed from the same infirm reasoning as its rejection of X's contract claim.

IV. Fourth, the district court erred in dismissing X's claim under the CFAA. X's complaint squarely alleges that CCDH fraudulently gained access to a protected computer and took valuable data stored there without paying for it. And the losses X sustained as a result of this unlawful access—tens of thousands of dollars spent investigating, assessing, and responding to the breach—are recoverable under the CFAA. The district court concluded otherwise only by disregarding both the plain text of the statute and binding precedent from this Court.

V. Fifth, the district court erred in concluding that it lacked personal jurisdiction over ECF. Where, as here, an out-of-forum defendant commits *in the forum* the precise tortious act that is the basis of the plaintiff's claims, it is subject to jurisdiction in that forum under settled legal principles. And even setting this threshold point aside, ECF's conduct was purposefully directed at the United States: it enabled and induced the breach of contract at issue by improperly transmitting its login credentials to CCDH *in the United States*, giving CCDH unauthorized access to X's data located *in the United States*, and causing tens of millions of dollars of damages to X *in the United States*. X's claims arise out of these contacts between

ECF and the forum, and it is reasonable to exercise jurisdiction over ECF to adjudicate them here.

VI. Finally, the district court erred in denying X leave to amend. The district court denied leave based on purported futility and delay, but the court's flyspecking of the two potential amendments X proposed wrongly jumped to merits conclusions about those proposed amendments, and there is no basis for the district court's speculation that "X Corp.'s desire to amend may well be based on a dilatory motive," 1-ER-69, given that X at no point delayed any aspect of the proceedings.

ARGUMENT

I. The District Court Erred in Applying California's Anti-SLAPP Statute to X's Claims Arising from Defendants' Non-Protected Conduct.

The district court took a wrong turn right out of the starting gate, taking a garden-variety contract- and tort-law case and transmogrifying it into a Free Speech case subject to California's anti-SLAPP statute. That state statute applies to claims "against a person arising from any act of that person in furtherance of the person's right of petition or free speech under the United States Constitution … in connection with a public issue." CAL. CIV. PROC. CODE § 425.16(b)(1). X has raised no such claim, and the anti-SLAPP statute has no bearing here.

The California Supreme Court has been clear about the limited contours of California's law: "[T]he mere fact that an action was filed after protected activity took place does not mean the action arose from that activity for the purposes of the

anti-SLAPP statute." *Park*, 393 P.3d at 908 (citation omitted). "Rather, a claim may be struck only if the speech or petitioning activity *itself* is the wrong complained of, and not just *evidence of liability*." *Id.* at 907 (emphasis added). "Put another way, a court focuses its anti-SLAPP analysis on the specific conduct that the claim is challenging." *Jordan-Benel v. Universal City Studios, Inc.*, 859 F.3d 1184, 1190 (9th Cir. 2017). The question is thus whether the Plaintiff "based" its claims "essentially" on "protected activity," in which case the anti-SLAPP framework applies, "or alternatively," simply "refer[s] to [protected] activity that is only incidental or *collateral* to the main thrust of the complaint." *Wang v. Wal-Mart Real Est. Bus. Tr.*, 63 Cal. Rptr. 3d 575, 589 (Cal. Ct. App. 2007) (emphasis added).

Here, X brings claims based on CCDH's unlawful access to and scraping of X's data, not CCDH's *later* decision to publish a report that mischaracterized the data it unlawfully accessed. *See generally* 1-ER-113–18. Thus, X based its claims on Defendants' wrongful, unprotected, non-expressive conduct—not on Defendants' later-in-time speech exploiting their wrongful conduct. It is of no moment that *after* committing the non-expressive conduct that forms the basis for X's claims, Defendants' wrongdoing was "thereafter communicated by means of speech." *Park*, 393 P.3d at 907. That distinction is critical, for a contrary interpretation would provide a constitutional shield against liability to those who engage in unlawful, harmful conduct simply by speaking about the wrongful conduct

after it has been committed. Nor is it relevant that CCDH's published reports revealing and manipulating the data it unlawfully accessed and scraped may create additional "evidence of liability." *Id.* For "the specific conduct that [X] is challenging," *Jordan-Benel*, 859 F.3d at 1190, is none of these things: instead, it is *only* Defendants' actions in unlawfully accessing and obtaining that private data in the first place. This is a critical distinction that precludes the application of the anti-SLAPP statute's special protections.

In its determination to transform this into a First Amendment case, the district court analogized Defendants' unlawful activities to "newsgathering." Under that doctrine, the California courts have found certain non-expressive conduct in investigating the news to be in furtherance of speech. *See, e.g.*, *Iloh v. Regents of Univ. of Cal.*, 312 Cal. Rptr. 3d 674, 682 (Cal. Ct. App. 2023). But the allegations in the complaint—which, again, must be taken as true at this stage—conclusively establish that CCDH did not scrape X to "report[] the news" at all. *Id.* X has plausibly alleged that CCDH is an activist organization that wrongfully accessed X's data, scraped that data, and manipulated that data, all with the goal of damaging X's commercial interests—not to report the news. Further, it is long settled that "[t]he right to speak and publish does not carry with it the unrestrained right to gather information." *Zemel v. Rusk*, 381 U.S. 1, 16–17 (1965).

In sum, Defendants did not satisfy "the[ir] burden of establishing that the challenged allegations or claims 'arise from' protected activity," so the district court's application of the anti-SLAPP framework was in error. *Park*, 393 P.3d at 907 (cleaned up). But even if the district court's framing of this case as a Free Speech case subject to the anti-SLAPP statute were correct, its decision striking the complaint must still be reversed, for an anti-SLAPP motion focused on legal sufficiency is merely subject to review under a Rule 12(b)(6) standard, *Planned Parenthood Fed'n of Am. v. Ctr. for Med. Progress*, 890 F.3d 828, 834 (9th Cir. 2018); *see* 1-ER-44, and X has plausibly alleged several claims for relief.

II. X Plausibly Alleged Breach of Contract.

X plausibly alleged breach of contract, and the district court erred in finding otherwise. "[T]he elements of a cause of action for breach of contract are (1) the existence of the contract, (2) plaintiff's performance or excuse for nonperformance, (3) defendant's breach, and (4) the resulting damages to the plaintiff." *Oasis W. Realty, LLC v. Goldman*, 250 P.3d 1115, 1121 (Cal. 2011). The district court did not dispute that X had plausibly alleged facts satisfying the first three elements, but the court nonetheless struck X's contract claim, concluding that X did not plausibly allege "recoverable damages." It based its conclusion both on federal constitutional law from the realm of defamation and on state contract law concerning "special damages." Both lines of reasoning were in error.

A. The District Court Erred in Importing Defamation Elements and Broader First Amendment Limitations onto X's Contract Claim.

The district court rejected X's damages allegations through a labeling exercise: it deemed X's breach-of-contract damages to be "reputational damages" subject to the First Amendment restrictions that apply to defamation claims—a type of claim *that X never even asserted*. That was error. Even assuming X's breach of contract claim can be read as implicating the First Amendment—and it cannot—the district court's novel theory finds no basis in any caselaw and in fact is foreclosed by binding precedent of this Court and the Supreme Court.

As discussed above, the First Amendment has no bearing here because X bases its breach of contract claims on Defendants' non-expressive conduct—scraping a website—not on any protected speech. That CCDH chose to speak *after* its breach to magnify the damage to X does not change that fundamental fact. The First Amendment standard for defamation suits is thus entirely irrelevant.

Indeed, the constitutional standard for defamation claims is also irrelevant because X has never asserted a defamation claim. The "plaintiff is the master of the plaintiff's complaint." *Hansen v. Grp. Health Coop.*, 902 F.3d 1051, 1056 (9th Cir. 2018). Yet the district court held that X failed to state a claim for *breach of contract* because it failed to satisfy the constitutional standards for *a tort claim it did not assert*.

In reality, labeling X's damages as "reputational harms" is misleading and contrary to the allegations in the complaint. X does not plead reputational harm or a broader loss of goodwill. Rather, X alleges that CCDH was successful in causing the economic damage it specifically and directly sought to cause through its breach—foreseeably resulting in X losing advertisers through CCDH's use of the data it accessed and scraped without authorization. This tight chain of causation places X's loss well outside the category of "reputational damages."

The Supreme Court's decision in *Cohen v. Cowles Media Co.*, 501 U.S. 663, 671 (1991), is directly on point and controlling. In *Cohen*, the plaintiff—a Republican political operative—sued two Minnesota newspapers for breach of promise. Cohen had provided the newspapers with documents relating to a candidate for Minnesota Lieutenant Governor on the condition that his involvement would be kept confidential, but the papers ultimately published his name in connection with the story. Cohen sued, and the Supreme Court held that he was entitled to recover compensatory damages for the publication *without having to satisfy* any First Amendment or defamation limitations.

The *Cohen* Court emphasized that Cohen was "*not* seeking damages for injury to his reputation or his state of mind." *Id.* (emphasis added). Rather, "[h]e sought damages in excess of $50,000 for breach of a promise that caused him to lose his job and lowered his earning capacity." *Id. Cohen* was thus "not a case like *Hustler*

Magazine, Inc. v. Falwell, 485 U.S. 46, [] (1988), where [the Court] held that the constitutional libel standards apply to a claim alleging that the publication of a parody was a state-law tort of intentional infliction of emotional distress." *Id.* For unlike cases involving tort law, in which "the State itself defined the content of publications that would trigger liability," principles of promissory estoppel merely enforce commitments in which *the parties* agreed to act in a way that could restrict speech. *Id*. at 670. "Minnesota law simply requires those making promises to keep them." *Id.* at 671. "The parties themselves . . . determine[d] the scope of their legal obligations, and any restrictions that may be placed on the publication of truthful information are self-imposed." *Id.*

As in *Cohen*, so too here. X's damages are just like those in *Cohen*—concrete and limited to specific economic losses that resulted from CCDH's breach of its promise. X *does not* seek "damages for injury to [its] reputation or . . . state of mind." *Id.* And X's damages arise from CCDH's breach of "legal obligations" that were "self-imposed." *Id.* Having freely entered contractual commitments not to scrape X's data, "[California] law simply requires [CCDH] to keep them." *Id.* Moreover, the fact that X's specific losses flow from CCDH's publication of reports that discuss issues of public concern is of no moment; for as *Cohen* explains, even members of the traditional, institutional press are not immune from laws of "general applicability" just because they engage in protected speech. *Id.* at 670. Just as

"[t]here can be little doubt that the Minnesota doctrine of promissory estoppel is a law of general applicability," *id.*, so too is there no doubt at all that the California law of contracts is a law of "general applicability." *Id*. CCDH cannot point to the First Amendment as nullifying its specific contractual commitments.

Cohen also expressly rejected the district court's assertion that recovering for breach of contract based on protected speech would "punish" speakers "for publishing truthful information that was lawfully obtained, "because compensatory damages are not a form of punishment." *Id.*; 1-ER-34 (asserting that this suit is "about punishing the Defendants for their speech"). The "characterization of the payment makes no difference for First Amendment purposes when the law being applied is a general law and does not single out the press." *Cohen*, 501 U.S. at 670.

This Court has also expressly rejected the district court's theory as foreclosed by *Cohen*. In *Planned Parenthood Federation of America v. Newman*, the Court rejected an "argument that, absent a showing of actual malice, all damages related to truthful publications are necessarily barred by the First Amendment." 51 F.4th 1125, 1134–35 (9th Cir. 2022), *cert. denied sub nom. Ctr. for Med. Progress v. Planned Parenthood Fed'n of Am.*, 144 S. Ct. 263 (Mem.) (2023). That argument, this Court held, "cannot be squared with *Cohen*." *Id*. After all, "[i]n *Cohen*, the Supreme Court upheld an economic damage award reliant on publication—damages

related to loss of earning capacity—even though the publication was truthful and made without malice." *Id.* (citing *Cohen*, 501 U.S. at 671).

The district court sought to sweep *Cohen* to the side by seizing upon a single line of dicta. After holding that the plaintiff could recover on a promissory estoppel claim for damages from publication, the *Cohen* Court remarked that "[n]or is Cohen attempting to use a promissory estoppel cause of action to avoid the strict requirements for establishing a libel or defamation claim." 501 U.S. at 671. The Court reasoned that Cohen "could not sue for defamation because the information disclosed [] was true," *id.*, and that he was "not seeking damages for injury to his reputation or his state of mind." *Id.* But X is *also* not seeking such damages. And the Court's reference to the unavailability of a defamation suit as evidence that Cohen was not attempting to circumvent the *New York Times v. Sullivan* standard obviously does not amount to a holding by implication that this standard applies not only to defamation claims but to all garden-variety contract claims whenever the plaintiff could conceivably *also* have pleaded defamation but chose not to.

Indeed, were it the law, the district court's attempted distinction of *Cohen* on the ground that the disclosure there involved truthful information not subject to a potential defamation claim, 1-ER-66, would create perverse results. It would put plaintiffs with a breach of contract claim for the improper disclosure of information in a worse position if the defendant lied as part of the disclosure than if the defendant

told the truth, because the plaintiff could recover on their breach of contract claim in the first scenario only by satisfying the actual malice standard but need only prove a standard breach of contract in the latter. That makes no sense.

Disregarding binding precedent, the district court instead invoked non-binding out-of-Circuit precedent and district court orders. *See* 1-ER-63–66. The district court relied primarily on *Food Lion, Inc. v. Cap. Cities/ABC, Inc.*, 194 F.3d 505 (4th Cir. 1999), in which the Fourth Circuit affirmed a district court's rejection of publication damages for non-reputational tort claims. But the Fourth Circuit's holding, to the extent it is persuasive, is distinguishable. First, the plaintiff there asserted tort claims, not a breach of contract. This is important because, as the Supreme Court emphasized in *Cohen*, a defendant can naturally and predictably be held to foresee the consequences of breaching the promises it makes. 501 U.S. at 671. When a defendant makes a binding promise, the defendant's liability in breaching its own promise is "self-imposed." *Id.* Second, the *Food Lion* plaintiff's asserted damages, including "loss of good will," 194 F.3d at 523, were more attenuated—and far more akin to the type of reputational damages sought in a defamation suit—than X's claim for the advertising revenue it lost on account of CCDH's effort *to reduce X's advertising revenue*. The district court's cited district court orders, 1-ER-63–66, are distinguishable for the same reason.

B. The District Court Misapplied State Contract Law.

Applying the right standard for the claim X actually brought, X has met its burden to allege damages under California contract law. X alleged with specificity that, as a direct result of CCDH's breach of the Terms of Service, certain companies that advertised on X paused their advertising spending, 1-ER-111–12, paused future plans for advertising, 1-ER-112, and paused plans to reactivate advertising campaigns, *id.* "CCDH engaged in its unlawful scraping with the intent to improperly obtain data that would be used to cause X Corp. to lose significant advertising revenues." 1-ER-113. The district court held that X was required to satisfy the heightened pleading requirements of Federal Rule of Civil Procedure 9 for "an item of special damage," but it plainly erred in concluding that X had not done so.

Special damages are "losses that do not arise directly" from the breach, but from "special or particular circumstances." *Lewis Jorge Constr. Mgmt., Inc. v. Pomona Unified Sch. Dist.*, 102 P.3d 257, 261 (Cal. 2004). "Special damages are recoverable if the special or particular circumstances from which they arise were actually . . . known by the breaching party (a subjective test) or were matters of which the breaching party should have been aware at the time of contracting (an objective test)." *Id.* X's advertising loss damages were not only foreseeable by CCDH—they were *actually foreseen* and in fact *intended.* CCDH engaged in

unauthorized scraping and accessing of data with the express purpose of calling for advertiser boycotts based on that data. CCDH cannot now claim that the damage *it specifically sought* was impossible to foresee.

Indeed, CCDH boasts a *sustained record* of scraping and manipulating data and causing harm to open social media fora. That is CCDH's modus operandi. As X alleges, "CCDH's underhanded conduct is nothing new. It has a history of using similar tactics not for the goal of combating hate, but rather to censor a wide range of viewpoints on social media with which it disagrees." 1-ER-120. "CCDH's efforts *often* rely on obtaining and intentionally mischaracterizing data." *Id*. (emphasis added). Further, CCDH specifically targets advertisers, conducting "scare campaign[s] to global advertisers" and asserting "ongoing pressure on brands." 1-ER-121. Thus, it was entirely predictable and well within CCDH's contemplation at the time of contracting that if it scraped data with the intent to harm X's advertising revenue, that it would *succeed* in harming X's advertising revenue.

The district court's contrary conclusion is premised on a basic analytical error. The court reasoned that "in 2019 [] Twitter looked quite different. Elon Musk had not yet taken over and turned Twitter into the X platform." 1-ER-58. The court thus reasoned that it was not "foreseeable" that the Twitter platform would later be changed in a way that would provoke CCDH to target X with one of its reports and boycott campaigns. *Id.* This confuses the foreseeability of a defendant's *decision to*

breach a contract with the foreseeability of the ensuing damages *caused by that decision*. The question in assessing damages is not whether the defendant contemplated *breaching* the contract at the outset; rather, the question is whether "the defendant should have contemplated the fact that [the alleged] *loss* would be 'the probable result' of the defendant's breach." *Lewis Jorge Constr. Mgmt.*, 102 P.3d at 262 (emphasis added). If the district court's foreseeability analysis were correct, special contract damages *would virtually never be recoverable*—even if they were explicitly spelled out in the contract itself. For very few contract partners start out expecting to breach a contract.

It more than plausibly follows from X's detailed allegations that CCDH—both in 2019 and during the subsequent years in which it continued to agree to the Terms of Service—should have contemplated that scraping X's data to discourage advertising on X would result in loss of advertising revenue for X.[2] Thus, X has satisfied any required showing of foreseeability of its damages.

[2] In any case, the district court's conclusion that CCDH could not have foreseen the sale of Twitter to Elon Musk is factually incorrect on its own terms. The district court asserted that, even if CCDH acknowledged updated terms of service by logging back into the platform after 2019 (which it must have done to access the site to scrape it), the terms of service CCDH breached were put in place in June 2022, which "predated Musk's purchase of Twitter." 1-ER-59. In fact, June 2022 was two months *after* Elon Musk's highly publicized agreement to buy Twitter and make changes to the platform in April 2022. *See, e.g.*, Mike Isaac & Lauren Hirsch, *With Deal for Twitter, Musk Lands a Prize and Pledges Fewer Limits*, N.Y. TIMES (Apr. 25, 2022), https://nyti.ms/3W92uiU.

To the extent the district court's decision turned on a requirement to disaggregate the specific sources of X's loss of advertising revenue, 1-ER-61–62, that holding is wrong for two reasons. First, X's specific allegations of special damages—including a specified source (loss of advertising revenue) and a specified amount (at least tens of thousands of dollars), satisfy the required Rule 9(g) showing, which only requires that damages be "specifically stated." FED. R. CIV. P. 9(g). By way of example, this Court has affirmed "special damages of $20,000," *Carrigan v. Cal. State Legislature*, 263 F.2d 560, 568 (9th Cir. 1959), and "Special Damages" including "$20,957.79 for lost wages," *Barnett v. Sea Land Serv., Inc*., 875 F.2d 741, 743 n.2 (9th Cir. 1989), without further breakdown. The district court cited no precedent of this Court for its supposition that more was required. X's allegations of lost advertising revenue from "eight [] specific organizations and companies" exceed the relatively low bar. 1-ER-112. Further X plausibly alleged *continuing* harm from Defendants' actions, 1-ER-111–13, which would of course become more specific after the complaint was filed as advertisers continued to decide to formally pull their advertising from X. Second, even if a *further* heightened standard applied, X could amend its complaint to provide yet more specificity. The district court's speculation that such an effort *may* prove "hard" for X, 1-ER-61, is no ground for dismissal. *See infra*, Part VI.

Finally, even apart from X's special damages for CCDH's breach of contract, X pleaded a separate and distinct category of damages that are indisputably "general," not "special," because they flow immediately and directly from CCDH's breach. General damages either "flow directly and necessarily from a breach of contract," or are a "natural result of a breach." *Lewis Jorge Constr. Mgmt.*, 102 P.3d at 261; *see also* CAL. CIV. CODE § 3300 (general damages "in the ordinary course of things, would be likely to result" from breach). Whether damages are "general" thus turns on whether the damages would have been reasonably "*within the contemplation of the parties*, meaning that because their occurrence is sufficiently predictable the parties at the time of contracting are 'deemed' to have contemplated them." *Lewis Jorge Constr. Mgmt.*, 102 P.3d at 261 (emphasis added). That said, "the parties need not 'actually have contemplated the very consequence that occurred.'" *Id.* (quoting *Hunt Bros. Co. v. San Lorenzo Water Co.*, 87 P. 1093, 1095 (Cal. 1906)).

X plausibly alleged that it incurred "additional losses" beyond the advertising loss damage CCDH intended to cause through its release of the improperly obtained data. These additional losses include, "[a]mong other things," the costs of conducting "internal investigations in efforts to ascertain the nature and scope of CCDH's unauthorized access to [X] data," "significant employee resources and time to participate and assist in those investigations," and "attorneys' fees and other costs

in aid of those investigations and in enforcing the relevant agreements, all of which were reasonably incurred in responding to CCDH's offense and/or conducting a damage assessment." 1-ER-112.

The district court relegated these well-pleaded factual allegations to a footnote. 1-ER-56 n.12. In the court's view, "those other sources of X Corp.'s damages appear in the complaint as allegations of harm caused by CCDH's unauthorized access to the [Brandwatch] data—something not at issue in the first cause of action." *Id.* (internal quotation marks omitted). But the district court was wrong to silo off these damages from X's breach of contract claim. Indeed, these allegations appear in the *very same section* of the complaint that discusses X's broader damages—immediately following X's allegations about loss of advertisers. And even if these allegations could properly be read as limited only to CCDH's "unauthorized access to data via Brandwatch"—despite the court's duty to construe any ambiguities in the complaint in X's favor at the pleading stage—CCDH's unauthorized access is inextricably linked to its scraping, which forms the basis of the breach of contract claim, because CCDH necessarily engaged in both acts in its efforts to reduce X's advertising revenue. *See* 1-ER-113 ("CCDH engaged in its unlawful scraping with the intent to improperly obtain data that would be used to cause X Corp. to lose significant advertising revenues."). Indeed, X's factual

allegations about additional damages *specifically reference the CCDH contract*. *See* 1-ER-112 (alleging costs incurred in "enforcing the relevant agreements").

The district court dismissed X's claims only by construing its damages allegations *against* it. This error was critical because even if the district court were right—which it is not—that X cannot recover for the advertising loss damages CCDH caused X through its improper scraping, these additional damages allegations are entirely independent of CCDH's alleged speech-related activities and preclude dismissal of X's breach of contract claim.

III. The CFAA Entitles X To Recover Costs Attributable to CCDH's Violations of the Statute.

The Computer Fraud and Abuse Act ("CFAA") is perhaps the Nation's most important cybersecurity statute. It prohibits individuals from accessing a "protected computer" without authorization. And it prescribes civil and criminal penalties when a person does so anyway. When a company "suffers damage or loss" because of a CFAA violation, it can bring a civil action against the violator to obtain "compensatory damages" and other appropriate relief. 18 U.S.C. § 1030(g).

CCDH violated the CFAA when it knowingly used another entity's login credentials to access a secure database containing X's nonpublic, proprietary data. CCDH knew that it was not authorized to access the database, but it did so anyway. And once inside, CCDH took the data without authorization.

When X learned about these potential violations of the CFAA, it launched an internal investigation to determine what was taken, who took it, and the extent of any damage. As detailed above, the company expended considerable resources responding to the breach and assessing potential damage. These expenditures are compensable "loss[es]" under the CFAA. 18 U.S.C. § 1030(e)(11).

Yet the district court dismissed X's claim. Departing from the teaching of this Court and other Circuits, the district court held that X failed to plead a qualifying "loss" under the CFAA because its injury was not sufficiently "technical" or "technological" in nature. 1-ER-78. That was error. The CFAA defines the term "loss" as "*any* reasonable cost to any victim"—expressly "including the cost of responding to an offense" and the cost of "conducting a damage assessment." 18 U.S.C. § 1030(e)(11) (emphasis added). Resources spent investigating and responding to CFAA violations are middle-of-the-fairway examples of "loss" under the statutory text, regardless of their technological nature. This Court should correct the district court's foundational error and reverse its dismissal of X's CFAA claim.[3]

[3] ECF conspired with CCDH to violate the Act, so it is also liable. *See* 1-ER-105, 114–15; 18 U.S.C. § 1030(b). Because the district court dismissed ECF on jurisdictional grounds and rejected X's primary CFAA claim against CCDH, it had no occasion to reach this issue.

A. CCDH Violated the CFAA When It Used Another Entity's Credentials To Access a Secured, Proprietary Database.

Before an entity can be held liable for causing a "loss" under the CFAA, that entity must have violated the CFAA. 18 U.S.C. § 1030(g). Here, X's complaint pleads such a violation.

An entity violates the CFAA when it "knowingly and with intent to defraud, accesses a protected computer without authorization . . . and by means of such conduct furthers the intended fraud and obtains anything of value." *Id.* § 1030(a)(4). A "protected computer" refers to any computer "used in or affecting interstate or foreign commerce or communication." *Id.* § 1030(e)(2)(B). This includes "effectively any computer connected to the Internet." *hiQ Labs, Inc. v. LinkedIn Corp.*, 31 F.4th 1180, 1195 (9th Cir. 2022) (holding that a server was a protected computer). And when one person uses another's credentials to gain unauthorized access to a protected computer, that person has accessed a protected computer "without authorization." *United States v. Nosal*, 844 F.3d 1024, 1038 (9th Cir. 2016).

In *Nosal*, the defendant had left his employer to start a competing business. *Id.* at 1030. He then conspired to access his former employer's confidential database—a "protected computer." And he did so using login credentials that belonged to his former executive assistant. *Id.* at 1029. This Court held that such unauthorized access was a "straightforward" violation of the CFAA. *Id.* at 1029–30.

So too here. X entered into a contract with Brandwatch, licensing certain non-public datasets to it. 1-ER-94–96, 106. These datasets were stored on Brandwatch's "protected servers in the United States," and X continuously "streamed" its data to these servers. 1-ER-94–95. The proprietary data was accessible only to approved users with "secure login credentials"—all others were strictly barred from accessing the data. 1-ER-94, 106.

CCDH lacked login credentials and was under no illusion that it had permission to access the protected data. 1-ER-106. Indeed, CCDH *knew* that it was not authorized to access the materials. 1-ER-98–99. CCDH also knew that other entities, such as ECF, were prohibited from sharing their login credentials with it. *Id.* Even so, CCDH obtained ECF's login credentials, 1-ER-99, and then used those credentials to gain unauthorized access to X's proprietary data. It did so on numerous occasions. And it did so knowing on each occasion that its access was unauthorized. 1-ER-92–101.

These facts thus state a textbook violation of CFAA, 18 U.S.C. § 1030(a)(4): CCDH knowingly and with fraudulent intent gained access to a protected computer. CCDH did so using another entity's credentials, even though it knew it was prohibited from doing so. And CCDH then used this fraudulently obtained access to take valuable data from the protected computer.

B. X Suffered a Loss as a Result of CCDH's Violation.

For civil liability to attach to a CFAA violation, two additional conditions must be met. First, a person must suffer "damage or loss" due to a violation of the Act. 18 U.S.C. § 1030(g). And second, the loss must total at least $5,000 in one year. *Id.* § 1030(a)(4); *see also id.* § 1030(c)(4)(A)(i)(I). The second condition is easily dispensed with here: X has pleaded losses that "amount to well over $5,000 aggregated over a one-year period." 1-ER-129. Indeed, the company incurred "tens of thousands of dollars" of expenses in connection with investigating the data breach, responding to CCDH's offense, and conducting a damage assessment. 1-ER-104. The primary question, then, is whether these losses count for purposes of the CFAA.

They plainly do. The term "loss" is broadly defined in the CFAA; it means "*any reasonable cost* to any victim, including *the cost of responding to an offense*, *conducting a damage assessment*, and restoring the data, program, system, or information to its condition prior to the offense, and any revenue lost, cost incurred, or other consequential damages incurred because of interruption of service." 18 U.S.C. § 1030(e)(11) (emphases added).

The damages alleged by X fit squarely within this definition. X conducted internal investigations into "the nature and scope of CCDH's unauthorized access." 1-ER-104. To perform these investigations, X expended "significant employee

resources and time." *Id.* The company also incurred attorneys' fees and other costs in support of its internal investigations and in connection with enforcing relevant data agreements. *Id.* These costs, the complaint plausibly explains, all occurred in connection with "responding to CCDH's offense" and "conducting a damage assessment." *Id.*; *see also* 18 U.S.C. § 1030(e)(11) (essentially verbatim).

Consistent with a straightforward reading of the CFAA's "loss" provision, this Court held in *Facebook, Inc. v. Power Ventures, Inc.*, that internal investigation expenses qualify as losses under the CFAA. 844 F.3d 1058, 1066 (9th Cir. 2016). In that case, a company continued to access Facebook after receiving a cease-and-desist letter. *Id.* at 1067. This Court held that Facebook employees' time spent "analyzing, investigating, and responding" to the company's unauthorized access qualified as "a loss under the CFAA." *Id.* at 1066. That reading of the "loss" provision—including its applicability to internal investigation costs—appears to be consistent with all other Circuits that have passed upon 18 U.S.C. § 1030(e)(11).

The First Circuit, for instance, holds that an expense qualifies as a "loss" under 18 U.S.C. § 1030(e)(11) if it "would not have been incurred in the absence of the offense." *United States v. Janosko*, 642 F.3d 40, 42 (1st Cir. 2011). Internal investigations and the other response costs that X has pleaded would surely qualify. Similarly, the Fourth Circuit has held that the CFAA's loss provision "plainly contemplates . . . costs incurred as part of the response to a CFAA violation,

including the investigation of an offense." *A.V. ex rel. Vanderhye v. iParadigms, LLC*, 562 F.3d 630, 646 (4th Cir. 2009) (emphasis added). And the Sixth Circuit agrees. In *Yoder & Frey Auctioneers, Inc. v. EquipmentFacts, LLC*, that court faced a situation where one company gained unauthorized access to another company's database using login credentials that were not its own. 774 F.3d 1065, 1069 (6th Cir. 2014). The Sixth Circuit held that costs "to investigate the offense and conduct a damage assessment" were "losses" under the CFAA. *Id.* at 1074. Finally, the Eleventh Circuit has likewise recognized that "losses" under the CFAA are "not limited to damage to a computer or network," but include "[t]he reasonable cost of responding to the offense." *Brown Jordan Int'l, Inc. v. Carmicle*, 846 F.3d 1167, 1175 n.2 (11th Cir. 2017).

In sum, X pleaded specific expenses that it incurred as a result of CCDH's violation of the CFFA. Those expenses count as "losses" under the plain meaning of 18 U.S.C. § 1030(e)(11).

C. The District Court Erred in Holding, Contrary to the CFAA's Unambiguous Text, that Only "Technological" Losses Count.

The district court reached a contrary conclusion only by venturing far from the statutory text of the CFAA's "loss" provision. The statute, again, defines a "loss" to include "*any reasonable cost* to any victim," "including the cost of responding to an offense" and the cost of "conducting a damage assessment." 18 U.S.C. § 1030(e)(11) (emphasis added). But the district court added a new requirement to

the statute—derived not from the CFAA's text but from two inapposite cases—that a "loss" only counts for purposes of the CFAA if it is "technological" in nature. 1-ER-78–79. Applying its new rule, the district court held that X failed to state a claim, reasoning that costs associated with conducting an internal investigation and paying attorneys to assess, investigate, and respond to a CFAA violation are not compensable because they are not "technological." 1-ER-78–80.

In reaching this conclusion, the district court never addressed this Court's holding that internal investigation and response costs *do* qualify as losses under the CFAA, *see Power Ventures, Inc.*, 844 F.3d at 1066, or similar holdings from the Fourth and Sixth Circuits, *Vanderhye*, 562 F.3d at 646; *Yoder*, 774 F.3d at 1074. Instead, the district court relied on two inapposite cases to forge its new rule. *See* 1-ER-78.

This first of those cases was *Van Buren v. United States*, 593 U.S. 374 (2021). The question presented in *Van Buren* concerned the meaning of the phrase "exceeds authorized access" in the CFAA. 18 U.S.C. § 1030(a)(2). The case did not concern the meaning of the CFAA's "loss" provision. *See id.* § 1030(e)(11). Indeed, neither of the parties' briefs even *cited* the provision, let alone analyzed it. Nor did the Eleventh Circuit's opinion below.

The Supreme Court briefly discussed the CFAA's damage and loss provisions. *See Van Buren*, 593 U.S. at 391–92. It did so in dicta to bolster its

structural argument that the phrase "exceeds authorized access" required an individual to exceed his or her ordinary technological permissions in a computer system. *Id*. The Supreme Court observed that the term "loss" "relate[d] to costs caused by harm to computer data, programs, systems, or information services," and it pointed out that the "statutory definition of 'damage' and 'loss' thus focus on technological harms." *Id*. But the Supreme Court did not say that *only* technological damages qualify as a "loss" under the CFAA. Rather, the Supreme Court—in support of a structural inference elsewhere in the statute—highlighted certain aspects of the CFAA's loss provision that specifically pertain to technological harms. *See* 18 U.S.C. § 1030(e)(11) (noting that certain technological harms qualify as CFAA losses, including "restoring the data, program, system, or information to its condition prior to the offense" and costs incurred due to "interruption of service"). The notion that the Court's passing reference rewrote and categorically limited the statute's loss provision to "technological" damages is untenable—especially in a case where the meaning of the CFAA's loss provision was neither presented nor briefed.

The other decision on which the district court relied was this Court's opinion in *hiQ Labs*, 31 F.4th 1180 (9th Cir. 2022). *See* 1-ER-78. That case is inapposite too. There, "the pivotal CFAA question" was "whether once hiQ received LinkedIn's cease-and-desist letter, any further scraping and use of LinkedIn's data was 'without authorization' within the meaning of the CFAA and thus a violation of . . . 18 U.S.C.

§ 1030(a)(2)"—even if the data was publicly available online. The Court determined that hiQ had "raised a serious question" concerning whether the phrase "'without authorization' limits the scope of the statutory coverage to computers for which . . . [something like] password authentication[] is generally required." *hiQ Labs*, 31 F.4th at 1197. And on this basis, the Court granted hiQ's motion for preliminary injunctive relief.[4]

In a short footnote, the Court quoted the technology-focused language from *Van Buren*, and it observed that LinkedIn had never alleged that hiQ's scraping of public profiles caused "technological harms." *Id.* at 1195 n.12. But that is where the Court left things. Its opinion contains no additional analysis of the CFAA's loss provision and does not mention the CFAA's loss provision at any other point. Nor does the opinion purport to base its grant of preliminary injunctive relief on that provision. Accordingly, the footnote is inapposite dictum.

The district court also made much of the fact that X's proprietary data was kept on Brandwatch's servers, not X's, suggesting that this somehow made X's loss non-technological and therefore non-actionable under the CFAA. 1-ER-79. But as

[4] The Court had previously determined that the balance of hardships tipped decisively in hiQ's favor, and that a preliminary injunction would be appropriate so long as hiQ could demonstrate "serious questions going to the merits." *hiQ Labs*, 31 F.4th at 1188 (citing *Alliance for the Wild Rockies v. Cottrell*, 632 F.3d 1127, 1135 (9th Cir. 2011)). Thus, the decision's precedential value is limited even for those issues that were addressed.

the complaint expressly alleges, X "streamed" *its* data to these servers. 1-ER-95. X's proprietary datasets were no less compromised because they were accessed through Brandwatch servers. Perhaps Brandwatch, too, could bring a claim based on CCDH's infiltration of its servers. But that is of no moment, since the CFAA does not limit a violator's liability to a single entity: "*any* victim" may seek compensation for "any reasonable cost." 18 U.S.C. § 1030(e)(11) (emphasis added). As the Eighth Circuit has held, the CFAA "does not restrict consideration of losses to only the person who owns the computer system"—"losses sustained by [a third party]" also count. *United States v. Millot*, 433 F.3d 1057, 1061 (8th Cir. 2006). The fact that X's datasets were streamed to Brandwatch servers does nothing to diminish X's CFAA claim.

IV. X Plausibly Alleged Intentional Interference with Contractual Relations and Inducing Breach of Contract.

The district court also erred in striking X's tort claims. X plausibly alleged that CCDH and ECF worked together to interfere with, and induce the breach of, X's contract with Brandwatch, and the district court concluded otherwise only by refusing to accept X's well-pleaded factual allegations as true and applying flawed reasoning.

Intentional interference with contractual relations requires: "(1) a valid contract between plaintiff and a third party; (2) defendant's knowledge of this contract; (3) defendant's intentional acts designed to induce a breach or disruption of the contractual relationship; (4) actual breach or disruption of the contractual relationship; and (5)

resulting damage." *United Nat'l Maint., Inc. v. San Diego Convention Ctr., Inc.*, 766 F.3d 1002, 1006 (9th Cir. 2014) (citation omitted). Inducement of breach is narrower and requires "more than a mere disruption": an "actual breach." *Spanish Broad. Sys., Inc. v. Grupo Radio Centro LA, LLC*, No. 2:16-cv-980, 2016 WL 11741137, at *7 (C.D. Cal. May 23, 2016).

X plausibly alleged each element of both claims. As detailed above, Brandwatch agreed not to reveal X data to third parties *and* to ensure that other parties also did not reveal X data to third parties. Meanwhile, ECF used its Brandwatch credentials to give CCDH unauthorized access to X data. That act—by definition—caused Brandwatch to breach its promise to X. First, "Defendants knew . . . [that] X Corp. must have contracts with Brandwatch, and that Brandwatch would be prohibited under the terms of [its contract with X] from providing access to unauthorized parties." 1-ER-108. Further, "Defendants' conduct prevented Brandwatch from performing under [its contract with X]" because "Brandwatch failed to secure the data . . . according to the terms of the agreements." *Id*. And "[a]s a direct and proximate result of Defendants intentionally interfering with [Brandwatch's contract with X Corp.], X Corp. has suffered monetary and other damages of at least tens of millions of dollars." *Id*. X similarly alleged the elements of inducing breach of contract. *See* 1-ER-109–110.

Despite X's extensive and specific allegations on each element, the district court reasoned that X had not plausibly alleged intent (which it referred to as causation) and

damages. 1-ER-82. The district court's reasoning misunderstands the nature of the relevant contractual provisions and ignores the allegations showing that X in fact made a *greater* causal showing than required.

The basic thrust of the district court's reasoning on causation was, in a turn of phrase it borrowed from the Defendants, that "the access did not cause the breach, the breach caused the access." 1-ER-83. In other words, the district court reasoned that Brandwatch's breach of its contract with X caused CCDH to access X's data, rather than the other way around. But that is plainly incorrect. Brandwatch agreed that it would "not allow others to[] . . . otherwise transfer or provide access to, in whole or in part, the Licensed Material to any third party." 1-ER-127. No breach by anyone is alleged to have occurred prior to CCDH's access. Only once ECF and CCDH conspired to provide CCDH (a third party) access to the Brandwatch "Licensed Material" did a breach occur. 1-ER-130–33. Thus Brandwatch's breach of contract would not have occurred but for CCDH getting unauthorized access to X's data. X thus squarely alleged that Defendants *necessarily caused* Brandwatch's breach. It is difficult to imagine a more direct causal link, and these allegations well exceed the showing required to plausibly allege intentional interference with contractual relations and inducing breach of contract. An intentional act that necessarily causes a breach is surely sufficient to plausibly allege an intentional act that induces a breach.

X also adequately alleged damages. The district court rejected X's allegations "on constitutional grounds," finding that "the same constitutional principle that prohibits X Corp. from recovering publication damages on its contract claim prohibit it from recovering publication damages on its non-defamation tort claims." 1-ER-83. For the same reasons discussed *supra*, this reasoning wrongly imports defamation standards onto X's non-defamation claims. Again, X did not raise a defamation claim, and it does not seek reputation damages. It thus makes no sense to hold X's non-defamation claims to the constitutional standards required for defamation. Were it otherwise, a defendant could absolve itself of tort liability simply by speaking about an already-committed wrong. Everyday examples bear this out. Imagine that CCDH had stolen a laptop from X's offices, instead of data, and then published the information it secured from the laptop in an online report. Surely, the First Amendment would not preclude CCDH's liability for conversion. Just so here. The constitutional standards unique to the defamation context do not apply and cannot be leveraged to *preclude* liability for a non-defamation tort based on CCDH's knowing inducement of a breach of contract to steal confidential data.

At the very least, even accepting the district court's novel imposition of defamation caselaw, the court was wrong to strike X's claims alleging "losses caused by CCDH's unauthorized access to data via Brandwatch" including, "[a]mong other things," the costs of X's "internal investigations," "significant employee resources and

time," and "attorneys' fees," all of which "as of the date of th[e] Amended Complaint, are in excess of tens of thousands of dollars and will continue to increase." 1-ER-112.

V. ECF Is Subject to Personal Jurisdiction.

The district court also erred in holding that it lacked personal jurisdiction over ECF. Under the Due Process Clause, a state court may exercise jurisdiction over a defendant if it has "certain minimum contacts with it such that the maintenance of the suit does not offend traditional notions of fair play and substantial justice." *Int'l Shoe Co. v. Washington*, 326 U.S. 310, 316 (1945) (internal quotation marks omitted). And where, as here, a defendant is not "subject to the personal jurisdiction of any state court of general jurisdiction," *Holland Am. Line Inc. v. Wartsila N. Am., Inc.*, 485 F.3d 450, 461 (9th Cir. 2007), and the claims against it arise out of federal law, Federal Rule of Civil Procedure 4(k)(2) authorizes the federal courts to assert "nationwide" jurisdiction over it so long as the assertion comports with this same minimum-contacts test—with the difference that "rather than considering contacts between the [defendant] and the forum state, [the courts] consider contacts with the nation as a whole." *Id*. at 462.

In cases sounding in tort, this Court ascertains whether sufficient minimum contacts support specific personal jurisdiction by asking whether "(1) the defendant purposefully direct[ed] its activities at the forum, (2) the lawsuit arises out of or relates to the defendant's forum-related activities, and (3) the exercise of jurisdiction

is reasonable." *Will Co. v. Lee*, 47 F.4th 917, 922 (9th Cir. 2022) (cleaned up). All three elements are met here.

A. ECF Purposefully Directed its Tortious Conduct at the United States.

"To determine whether a defendant purposefully directed its activities at the forum," this Court asks, "whether the defendant: (1) committed an intentional act, (2) expressly aimed at the forum [country], (3) causing harm that the defendant knows is likely to be suffered in the forum [country]." *Id.* (cleaned up). The district court correctly held that the first and third prongs of this test were met, but it concluded that X had "not adequately alleged that ECF expressly aimed its activities at the United States." 1-ER-24. Because the tortious act that gave rise to X's claims against ECF *itself occurred in the United States* and was part of a course of conduct that was *expressly aimed* at the United States, ECF's actions were purposefully directed here.

1. ECF Is Subject to Jurisdiction Because It Committed the Tortious Act at Issue in the United States.

The determination whether a court can constitutionally assert specific personal jurisdiction "focuses on the relationship among the defendant, the forum, and the litigation." *Walden v. Fiore*, 571 U.S. 277, 284 (2014) (cleaned up). In cases where "allegedly tortious conduct takes place *outside* the forum and has effects inside the forum," *AMA Multimedia, LLC v. Wanat*, 970 F.3d 1201, 1208 (9th Cir.

2020), the minimum-contacts analysis can be difficult, as it involves a complex weighing of the extent and significance of the defendant's contacts with the forum.

This is not one of those cases. Instead, this case involves the situation where "a defendant engages in tortious activity toward a plaintiff in the state where that plaintiff resides." *Morrill v. Scott Fin. Corp.*, 873 F.3d 1136, 1148 (9th Cir. 2017). And in that situation, it is a "well-established rule" that "the defendant is subject to personal jurisdiction there." *Id.*

On a motion to dismiss for lack of personal jurisdiction, "[u]ncontroverted allegations in the complaint must be taken as true," *Will Co.*, 47 F.4th at 921, and here X's complaint squarely alleges that ECF "intentionally reach[ed] into the United States" by "wrongfully sharing its login credentials with CCDH US," 1-ER-95—a United State corporation "with its principal place of business in Washington D.C." 1-ER-97. The complaint was unambiguous about where the conduct occurred, alleging that ECF

> on several occasions since at least early 2021 agreed with CCDH to share its login credentials to enable CCDH's illegal access to the X Corp. data. . . . ECF knowingly and intentionally chose to unlawfully share its login credentials with a US entity, headquartered and operating from the United States.

1-ER-105.

ECF's sharing its Brandwatch login credentials with CCDH US in the United States is not an act of marginal significance to this case; it is *the very act* that violated

the CFAA, interfered with X's contract with Brandwatch, and induced CCDH to breach that contract. At bottom, ECF's transmittal of its login credentials to CCDH in the United States *is* its tort against X. Asserting jurisdiction over ECF in the United States thus no more offends due process than asserting jurisdiction over a defendant sued for "throwing a rock through a window of the plaintiff's residence in the forum state." *Morrill*, 873 F.3d at 1148. For as this Court has explained, it is a "well-established rule . . . that, when a defendant engages in tortious activity toward a plaintiff in the [forum] where that plaintiff resides, the defendant is subject to personal jurisdiction there." *Id.*; *see also Freestream Aircraft (Bermuda) Ltd. v. Aero Law Grp.*, 905 F.3d 597, 601, 603–04 (9th Cir. 2018) ("[g]enerally, the commission of an intentional tort in a state is a purposeful act that will satisfy the first two requirements of the minimum contacts test" and "[t]he district court's reliance on the *Calder* effects test" rather than "the location of [the] allegedly intentional tortious conduct" was "misplaced . . . because the inquiry under that test focuses on conduct that takes place *outside* the forum state and that has effects inside the forum state" (cleaned up)).

The case that this Court cited in *Morrill* for this "well-established rule," *Brainerd v. Governors of the University of Alberta*, 873 F.2d 1257 (9th Cir 1989), is instructive. In *Brainerd*, a professor at the University of Arizona sued his former employer, the University of Alberta, Canada, over making three "communications

to and from the University of Arizona regarding the rumors surrounding Brainerd's departure" from the University of Alberta, which caused him harm in Arizona. *Id.* at 1258–59. Those communications included "two telephone calls" and a letter. *Id.* at 1259. This Court held that "[t]hose contacts with the forum support personal jurisdiction," reasoning that the "communications were directed to Arizona, even though [the defendant] did not initiate the contact." *Id.*; *see also DEX Sys., Inc. v. Deutsche Post AG*, 727 F. App'x 276, 278 (9th Cir. 2018) ("Though [the defendants] certainly had limited contacts with California, [those] contacts include the allegedly tortious conduct in California that gave rise to DEX's claims. In such circumstances, limited contacts are sufficient to create jurisdiction."); *Alejandro Fernandez Tinto Pesquera, S.L. v. Fernandez Perez*, No. 20-cv-2128-LHK, 2021 WL 254193, at *10 (N.D. Cal. Jan. 26, 2021); *InfoSpan, Inc. v. Emirates NBD Bank PJSC*, No. 8:11-cv-1062, 2014 WL 12700983, at *5–6 (C.D. Cal. Apr. 10, 2014).

So too here. Whether ECF unlawfully conveyed its Brandwatch login credentials to CCDH by email, by letter, or by hand-delivery makes no practical difference—the key fact is that the credentials were conveyed *in the United States*. And all of X's "cause[s] of action arise[] from that [act]." *Freestream Aircraft*, 905 F.3d at 603. ECF is thus subject to jurisdiction under the "well-established rule . . . that, when a defendant engages in tortious activity toward a plaintiff in the [forum]

where that plaintiff resides, the defendant is subject to personal jurisdiction there." *Morrill*, 873 F.3d at 1148.

The district court's principal response to this basis for jurisdiction was to deny its premise: that ECF's credentials were shared with CCDH *in the United States*. The court attempted to avoid X's express allegations to that effect by pointing to a declaration submitted by one of ECF's officers, Morgan Després, who attached a copy of "a May 12, 2022 email chain . . . in which Brandwatch UK's senior customer service manager"—located in London—"facilitates Brandwatch account access" for an email address "belonging to Callum Hood"—who is allegedly "based in the UK and employed by CCDH UK." 1-ER-93. Nothing in this affidavit, or the attached email chain, contradicts X's unambiguous allegation that ECF shared its credentials with CCDH in the United States.

X squarely alleged that ECF "agreed with CCDH to share its login credentials" "*on several occasions*." 1-ER-105 (emphasis added). Propounding a cherry-picked excerpt of only one of those occasions from a single email chain between a Brandwatch employee and a CCDH employee working outside the United States does not and logically cannot establish that ECF did not transmit its credentials to CCDH in the United States *on another occasion*. Indeed, the email chain attached to Després's declaration is self-evidently *not part of ECF's transmittal of login credentials to CCDH at all*; rather, it is a fragment of a longer,

ongoing course of communication between CCDH and Brandwatch (not ECF), over the *use* of credentials that ECF *had already provided*. Notably, ECF was silent as to the other occasions on which it shared login credentials with CCDH, and ECF *never* unequivocally asserted, let alone evidenced, in the district court that it *did not* provide credentials to CCDH in the United States: Després tellingly avers nothing of the kind. 1-ER-91–93.

None of this contradicts X's express allegations that ECF conveyed its login credentials in the United States, so those allegations are "[u]ncontroverted" and "must be taken as true." *Will Co.*, 47 F.4th at 921. The district court's refusal to accept X's uncontroverted allegations for purposes of the motion to dismiss was an error of the plainest kind. It attempted to justify its departure from this basic procedural rule by suggesting that "[c]onflicts in the evidence are resolved in the plaintiff's favor only if the plaintiff submits admissible evidence," 1-ER-17, but that proposition is utterly irrelevant here, since *there is no conflict in the evidence*. Again, nothing ECF's declarant said actually contradicts X's well-pleaded allegation that it shared its login credentials with CCDH in the United States.

The district court's criticism of X for failing to back up its allegations on this point with "admissible evidence," *id*., comes with especially poor grace given that the court simultaneously *refused to grant X jurisdictional discovery*, based on the conclusory assertion that "discovery would not demonstrate facts sufficient to

constitute a basis for jurisdiction." 1-ER-32. Even if the Després declaration could be read as affirmatively stating that ECF never transmitted its login to the United States (and it cannot), X could only conceivably lay hands on "admissible evidence" contradicting that claim through the discovery process. The district court's catch-22 decision disregarding X's well-pleaded allegations by crediting its misreading of the Després declaration as uncontradicted, even as it refused to allow X to seek admissible evidence that would contradict it, was beyond the pale.

The court below also sought to wave away ECF's conduct in the United States by suggesting that it was not substantial enough, reasoning that "[i]t is hard to see the sharing of login credentials alone as enough to create a relationship to the forum state." 1-ER-18; *see also* 1-ER-19, 23. But the existence of jurisdiction here does not turn on whether sharing login information is "substantial" in some metaphysical sense. It turns on the fact that ECF "engage[d] in tortious activity toward [the] plaintiff in the state where that plaintiff resides." *Morrill*, 873 F.3d at 1148; *see DEX Sys.*, 727 F. Appx. at 278 ("In such circumstances, limited contacts are sufficient to create jurisdiction."). In the context of this case, ECF's transmission of login credentials plays the most "substantial" role possible: *it is the very tortious act giving rise to X's claims*.

2. ECF Is Subject to Jurisdiction Because its Tortious Conduct Was Expressly Aimed at the United States.

ECF is subject to personal jurisdiction even setting aside the "well-established rule" that committing a tortious act within the forum suffices to vest that forum's courts with jurisdiction. *Morrill*, 873 F.3d at 1148. ECF's course of conduct was directed at the United States in three ways—which, taken together, show that ECF "expressly aimed" its activity at the forum and is subject to jurisdiction here.

First, as just discussed, ECF shared its login credentials with CCDH in the United States. Even if that act does not establish personal jurisdiction on its own (and it does), it is still evidence that ECF's actions were aimed at the United States. And importantly, this act constitutes "suit-related conduct" creating a "connection with the forum" that is *independent* of the plaintiff's own conduct. *Walden*, 571 U.S. at 284–86. ECF's transmission of login credentials into the United States has nothing to do with X's own location here, and it establishes that X itself is not "the only link between the defendant and the forum." *Id.* at 285.

Second, ECF's provision of login credentials allowed, and was designed to allow, CCDH to access X's information on Brandwatch servers *located in the United States*. *See, e.g.*, 1-ER-98, 104, 120. The fact that the data that ECF improperly enabled CCDH to access was itself located in the United States constitutes a substantial connection with the forum. And once again, this connection is entirely independent of X's own location here—contrary to what the court below thought,

Brandwatch's location of its servers in the United States simply has nothing to do with the fact that "X Corp.'s principal place of business is in California." 1-ER-21.

The court below disregarded the location of the data at issue, citing several district-court cases for the proposition that "[t]he mere location of servers cannot establish personal jurisdiction." *Id.* But all of the cases it cited deal with servers that "were incidental to the alleged conduct" because they "were not the ultimate target of the [defendant's] intentional act." *WhatsApp Inc. v. NSO Grp. Techs. Ltd.*, 472 F. Supp. 3d 649, 671–72 (N.D. Cal. 2020), *aff'd on other grounds*, 17 F.4th 930 (9th Cir. 2021). The tortious acts in these cases utilized data that happened to incidentally be located in the forum, but the acts themselves were aimed elsewhere.

Here, by contrast, CCDH's conduct in accessing X's data stored on Brandwatch's servers in the United States is not "incidental to the alleged conduct" that gives rise to X's claims; *it is the conduct that gives rise to those claims*. *Id.* at 672. For unlike in the cases relied upon by the district court, X's claims all center *on CCDH's unlawful access itself*. This case is thus akin to *WhatsApp*, where the claims involved the defendant's transmission of malware to the plaintiff's servers in California. Because those claims "center[ed] on the improper access to and misuse of" the plaintiff's servers, the court reasoned that "[t]he location of the servers is, therefore, not a fortuity but central to the alleged tortious conduct." *Id.* at 670, 672. The fact that the data ECF improperly enabled CCDH to access was stored on

Brandwatch's servers in the United States is a substantial connection to the forum under the same reasoning.

Third, the complaint alleges that ECF's actions improperly providing CCDH with access to X's data through Brandwatch were a catalytic part of a larger, coordinated campaign that caused X tens of millions of dollars of losses *in California*. 1-ER-87–88, 90. ECF thus "individually targeted" X in the United States by "engag[ing] in wrongful conduct targeted at [X,] whom [ECF] knows to be a resident of the forum state." *Axiom Foods, Inc. v. Acerchem Int'l, Inc.*, 874 F.3d 1064, 1069 (9th Cir. 2017) (citation omitted). While the Supreme Court's decision in *Walden* makes clear that such "individual targeting" cannot establish jurisdiction "without more," this Court has held that it "may remain relevant to the minimum contacts inquiry." *Id.* at 1070. And here, there is much more: ECF's individual targeting of X in the United States is accompanied by (1) its provision of its Brandwatch login credentials to CCDH in the United States, which (2) allowed CCDH to improperly access X's data stored in the United States. Taken together, these connections to the forum establish that ECF's conduct was expressly aimed at the United States.

B. X's Claims Arise out of ECF's Contacts.

While a defendant's contacts with the forum will support specific jurisdiction only if the plaintiff's claims "arise out of or relate to" those contacts, the Supreme

Court has rejected any requirement that there be a "strict causal relationship" between the claims and the in-state contacts. *Ford Motor Co. v. Mont. Eighth Jud. Dist. Ct.*, 592 U.S. 351, 359, 362 (2021) (citation omitted). And here, ECF's contacts *satisfy* the causal relationship that the Court *rejected as too onerous*. As discussed above, ECF's provision of login credentials to CCDH in the United States, and the use of those credentials to improperly access data stored by Brandwatch in the United States, are the very basis of X's claims against ECF. Had those acts not happened, *X's claims would not exist*. Likewise, had those acts not caused significant damage to X in the United States, *X's claims would not exist*. *See* 1-ER-51 (noting that X's claims "require as an element a showing of damages").

The district court's decision to the contrary is plainly wrong. It again asserted that "ECF's evidence shows that ECF shared its login credentials with CCDH U.K.," rather than CCDH U.S., 1-ER-25, but as explained above, ECF's evidence showed nothing of the kind, and the court had no basis for disregarding X's uncontroverted allegation that the credentials were shared in the United States. The court below also stated that "ECF's sharing of login information is not connected to the United States, other than that X Corp. is located there," *id.*, but again, that is simply not so. Again, the fact that ECF improperly shared its login credentials with CCDH *in the United States* is wholly independent of X's location, as is the fact that ECF purposely enabled CCDH to improperly access data stored in the United States.

C. Asserting Jurisdiction over ECF Is Reasonable.

Finally, ECF cannot bear its burden of presenting "a compelling case that the exercise of jurisdiction would be unreasonable and therefore violate due process." *Ayla, LLC v. Alya Skin Pty. Ltd.*, 11 F.4th 972, 983–84 (9th Cir. 2021) (cleaned up). The inquiry into reasonableness is "guided by seven factors":

> (1) the extent of the defendant's purposeful interjection into the forum state's affairs; (2) the burden on the defendant of defending in the forum; (3) the extent of conflict with the sovereignty of the defendant's state; (4) the forum state's interest in adjudicating the dispute; (5) the most efficient judicial resolution of the controversy; (6) the importance of the forum to the plaintiff's interest in convenient and effective relief; and (7) the existence of an alternative forum.

Id. at 984 (quoting *Freestream Aircraft*, 905 F.3d at 607). The district court correctly held that the third, fourth, and sixth factors weigh in favor of jurisdiction. 1-ER-28–29. But the court nonetheless concluded that "more of the factors weigh in favor of ECF than X Corp." 1-ER-30. That was error. In fact, the remaining factors either favor jurisdiction or are insignificant, and jurisdiction would plainly be reasonable.

The district court's conclusion regarding the first factor, purposeful interjection, was based entirely on its earlier determination—under the "purposeful direction" prong of the analysis—that ECF "did not conduct activities that were ongoing and substantial" in the United States. 1-ER-27. But as shown above, ECF's connection with the forum *is* substantial: it committed the pivotal tortious act that gave rise to X's claims—improperly sharing its login credentials—*in the United*

States, so that CCDH could unlawfully access X's data stored *in the United States*, causing X tens of millions of dollars of damage *in the United States*.

With respect to the second and fifth factors, the burden on the defendant and most efficient judicial resolution, the district court held that litigating in the United States would be both burdensome for ECF and inefficient for the courts based on the notion that "ECF exclusively operates in Europe while X Corp. is a global company with offices in both Europe and the U.S." 1-ER-27. But this formalistic comparison of corporate letterheads ignores the practical realities of litigation: ECF's tortious acts, and the damage they inflicted on X, all occurred in the United States, and so X's witnesses and evidence are principally located here. In all events, as the district court conceded, these factors have little weight today, since "modern advances in communications and transportation have significantly reduced the burden of litigating in another forum," and indeed ECF is represented by a sophisticated U.S. law firm. *Id*. (quoting *Freestream Aircraft*, 905 F.3d at 608); *see also* 1-ER-28. The court erred in giving these factors any appreciable weight against the exercise of jurisdiction.

Finally, as to the seventh factor, the court below concluded that "an alternative forum exists in the U.K. or the Netherlands." 1-ER-30. But even if that is so, "whether another reasonable forum exists becomes an issue only when the forum state is shown to be unreasonable." *Ayla*, 11 F.4th at 984 (cleaned up). And since

ECF has fallen far short of making that showing, the court erred in giving this factor independent weight "in favor of ECF," 1-ER-30.

To find a violation of due process based on reasonableness, the jurisdictional analysis requires the defendant to make a "compelling case" against jurisdiction, *Ayla*, 11 F.4th at 979, not a milquetoast showing that "more of the factors weigh in favor of" declining jurisdiction as a bare numerical matter, 1-ER-30. ECF has made no such compelling case, and the district court erred in concluding that exercising jurisdiction would be unreasonable.

VI. The District Court Erred In Denying Leave to Amend.

Finally, in another remarkable ruling, the district court denied X leave to amend its complaint to address personal jurisdiction or any alleged deficiencies in X's claims. A district court should "freely" give leave to amend whenever "justice so requires." FED. R. CIV. P. 15(a)(2). "This policy is to be applied with extreme liberality." *Eminence Cap., LLC v. Aspeon, Inc.*, 316 F.3d 1048, 1051 (9th Cir. 2003) (internal quotation marks omitted). A district court may deny leave to amend if it finds undue delay, bad faith or dilatory motive, repeated failure to cure deficiencies after amendment was allowed, undue prejudice to the opposing party, or futility of

amendment. *Leadsinger, Inc. v. BMG Music Publ'g*, 512 F.3d 522, 532 (9th Cir. 2008).

Here, the district court "believe[d] that amendment would be futile," and opined that "X Corp.'s desire to amend may well be based on a dilatory motive." 1-ER-69. Neither explanation can justify the denial of leave to amend. As to futility, this Court will only affirm a "district court's dismissal on this basis [of futility] if it is clear, upon *de novo* review, that the complaint could not be saved by *any* amendment." *Leadsinger*, 512 F.3d at 532 (emphasis added) (internal quotation marks omitted). That high bar is not met here. The court concluded that X's two sets of proposed amendments did not "make very much sense," 1-ER-70, and made substantive conclusions about the truth of X's proposed allegations, *see* 1-ER-71, but this premature merits analysis—unmoored from the standards of Rule 12(b)(6)—is no basis for denying an opportunity to amend. In any case, X's proposed allegations concerning the data security implications of Defendants' wrongful acts and further descriptions of the harmful effects of CCDH's scraping are highly relevant. Both sets of allegations go directly to recoverable damages, which was the district court's basis for dismissal of X's breach of contract and tort claims. The district court was thus wrong to dismiss these amendments out of hand.

As to delay, the district court's reasoning was not actually based on delay at all, but rather on its own value judgment of X's suit: "It would be wrong to allow X

Corp. to amend again when the damages it now alleges, and the damages it would like to allege, are so problematic, and when X Corp.'s motivation is so clear." 1-ER-76. Needless to say, this expression of personal sentiment is no basis for a finding of delay. And no valid basis exists. X filed its initial complaint on July 31, 2023, and it requested leave to amend, in the alternative to dismissal with prejudice, on December 12, 2023—a little over 4 months later.

Finally, the district court also wrongly struck X's claims against Doe Defendants without leave to amend. Because X requires discovery to learn additional information about Doe Defendants' covert activities, it naturally follows that specificity will come with additional information revealed in discovery.

Although X's well-pleaded claims should not have been struck or dismissed in the first place, X should at the very least have an opportunity to amend.

CONCLUSION

For the foregoing reasons, this Court should reverse.

July 5, 2024 Respectfully submitted,

James Jonathan Hawk McDermott Will & Emery 2049 Century Park East Suite 3200 Los Angeles, CA 90067 (310) 788-4181 jhawk@mwe.com	/s/Charles J. Cooper Charles J. Cooper David H. Thompson Peter A. Patterson John D. Ohlendorf Samuel D. Adkisson Athanasia O. Livas Cooper & Kirk, PLLC

	1523 New Hampshire Avenue, N.W. Washington, DC 20036 (202) 220-9600 ccooper@cooperkirk.com
Attorneys for Plaintiff-Appellant X Corp.	

UNITED STATES COURT OF APPEALS
FOR THE NINTH CIRCUIT

Form 8. Certificate of Compliance for Briefs

Instructions for this form: http://www.ca9.uscourts.gov/forms/form08instructions.pdf

9th Cir. Case Number(s) 24-2643

I am the attorney or self-represented party.

This brief contains 13,919 **words,** including 0 words manually counted in any visual images, and excluding the items exempted by FRAP 32(f). The brief's type size and typeface comply with FRAP 32(a)(5) and (6).

I certify that this brief *(select only one)*:

- (●) complies with the word limit of Cir. R. 32-1.
- ( ) is a **cross-appeal** brief and complies with the word limit of Cir. R. 28.1-1.
- ( ) is an **amicus** brief and complies with the word limit of FRAP 29(a)(5), Cir. R. 29-2(c)(2), or Cir. R. 29-2(c)(3).
- ( ) is for a **death penalty** case and complies with the word limit of Cir. R. 32-4.
- ( ) complies with the longer length limit permitted by Cir. R. 32-2(b) because *(select only one)*:
  - [ ] it is a joint brief submitted by separately represented parties.
  - [ ] a party or parties are filing a single brief in response to multiple briefs.
  - [ ] a party or parties are filing a single brief in response to a longer joint brief.
- ( ) complies with the length limit designated by court order dated [ ].
- ( ) is accompanied by a motion to file a longer brief pursuant to Cir. R. 32-2(a).

Signature /s/Charles J. Cooper **Date** 07/05/2024

(use "s/[typed name]" to sign electronically-filed documents)

STATUTORY ADDENDUM

TABLE OF CONTENTS

Page

Computer Fraud and Abuse Act, 18 U.S.C. § 1030

(a) Whoever—

. . . .

(2) intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains—

(A) information contained in a financial record of a financial institution, or of a card issuer as defined in section 1602(n) of title 15, or contained in a file of a consumer reporting agency on a consumer, as such terms are defined in the Fair Credit Reporting Act (15 U.S.C. 1681 et seq.);

(B) information from any department or agency of the United States; or

(C) information from any protected computer;

. . . .

(4) knowingly and with intent to defraud, accesses a protected computer without authorization, or exceeds authorized access, and by means of such conduct furthers the intended fraud and obtains anything of value, unless the object of the fraud and the thing obtained consists only of the use of the computer and the value of such use is not more than $5,000 in any 1-year period;

. . . .

(b) Whoever conspires to commit or attempts to commit an offense under subsection(a) of this section shall be punished as provided in subsection (c) of this section.

(c) The punishment for an offense under subsection (a) or (b) of this section is—

. . . .

(4)(A) except as provided in subparagraphs (E) and (F), a fine under this title, imprisonment for not more than 5 years, or both, in the case of—

(i) an offense under subsection (a)(5)(B), which does not occur after a conviction for another offense under this section, if the offense caused (or, in the case of an attempted offense, would, if completed, have caused) —

(I) loss to 1 or more persons during any 1-year period (and, for purposes of an investigation, prosecution, or other proceeding brought by the

United States only, loss resulting from a related course of conduct affecting 1 or more other protected computers) aggregating at least $5,000 in value;

. . . .

(e) As used in this section—

. . . .

(2) the term "protected computer" means a computer—

. . . .

(B) which is used in or affecting interstate or foreign commerce or communication, including a computer located outside the United States that is used in a manner that affects interstate or foreign commerce or communication of the United States; or

. . . .

(11) the term "loss" means any reasonable cost to any victim, including the cost of responding to an offense, conducting a damage assessment, and restoring the data, program, system, or information to its condition prior to the offense, and any revenue lost, cost incurred, or other consequential damages incurred because of interruption of service;

. . . .

(g) Any person who suffers damage or loss by reason of a violation of this section may maintain a civil action against the violator to obtain compensatory damages and injunctive relief or other equitable relief. A civil action for a violation of this section may be brought only if the conduct involves 1 of the factors set forth in subclauses[4] (I), (II), (III), (IV), or (V) of subsection (c)(4)(A)(i). Damages for a violation involving only conduct described in subsection (c)(4)(A)(i)(I) are limited to economic damages. No action may be brought under this subsection unless such action is begun within 2 years of the date of the act complained of or the date of the discovery of the damage. No action may be brought under this subsection for the negligent design or manufacture of computer hardware, computer software, or firmware.

. . . .

Anti-SLAPP Law, CAL. CODE CIV. P. § 425.16

. . . .

(b)(1) A cause of action against a person arising from any act of that person in furtherance of the person's right of petition or free speech under the United States Constitution or the California Constitution in connection with a public issue shall be subject to a special motion to strike, unless the court determines that the plaintiff has established that there is a probability that the plaintiff will prevail on the claim.

. . . .