IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF TEXAS
DALLAS DIVISION

AT&T SERVICES, INC., and AT&T MOBILITY LLC, Plaintiffs, v. T-MOBILE US INC., Defendant.	Case No. 3:25-cv-03279-S **JURY TRIAL DEMANDED**

AT&T'S BRIEF IN SUPPORT OF ITS MOTION FOR TEMPORARY RESTRAINING ORDER AND PRELIMINARY INJUNCTION

TABLE OF CONTENTS

Page

I. INTRODUCTION 1
II. FACTUAL BACKGROUND 3
A. AT&T's Protection Of Consumer Data And Terms Of Use 3
B. T-Mobile's "Switch Made Easy" Relies On Bots Scraping AT&T's Websites 4
C. AT&T's Detection Of T-Mobile's Scraping Tool and Pre-Litigation Response 5
III. LEGAL STANDARD 7
IV. ARGUMENT 7
A. AT&T Is Likely to Succeed On Each Of Its Claims 8
1. Count I: Computer Fraud and Abuse Act, 18 U.S.C. § 1030(a)(2), (a)(4) 8
2. Count II: Tex. Comp. Crimes, Tex. Penal Code § 33.02, Civil Code § 143.001 12
3. Count III: Cal. Computer Data Access and Fraud Act, Cal. Penal Code § 502 13
4. Count IV: Georgia Computer Systems Protections Act, O.C.G.A. § 16-9-93 14
5. Count V: Breach of Contract 15
6. Count VI: Tortious Interference With Contract 17
B. AT&T Has And Will Suffer Immediate, Irreparable Harm 19
C. The Balance Of Equities Favors Granting Immediate Injunctive Relief 23
D. The Public Interest Favors Granting Immediate Injunctive Relief 24
V. CONCLUSION 25

TABLE OF AUTHORITIES

Page(s)

Cases

ACI Payments, Inc. v. Conservice, LLC,
No. 121CV00084RJSCMR, 2022 WL 622214 (D. Utah Mar. 3, 2022) 9

Allied Mktg. Grp., Inc. v. CDL Mktg., Inc.,
878 F.2d 806 (5th Cir. 1989) 19

Am. Airlines, Inc. v. Red Ventures LLC,
No. 4:22-CV-0044-P, 2022 WL 2790643 (N.D. Tex. July 15, 2022) 8

Am. Eyewear, Inc., v. Peeper's Sunglasses & Acc., Inc.,
106 F. Supp. 2d 895 (N.D. Tex. 2000) 17

Amigo Broad., LP v. Spanish Broad. Sys., Inc.,
521 F.3d 472 (5th Cir. 2008) 17, 18

Andra Grp., LP v. BareWeb, Inc.,
No. 4:17-CV-00815, 2018 WL 2848985 (E.D. Tex. June 11, 2018) 16

Atl. Recording Corp. v. Anderson,
No. CIVA H-06-3578, 2008 WL 2316551 (S.D. Tex. Mar. 12, 2008) 23

Barnstormers, Inc. v. Wing Walkers, LLC,
No. EP-10-CV-261-KC, 2011 WL 1671641 (W.D. Tex. May 3, 2011) 11

Biden v. Ziegler,
737 F. Supp. 3d 958 (C.D. Cal. 2024) 13

CDK Glob., LLC v. Tekion Corp.,
No. 25-CV-01394-JSC, 2025 WL 1939951 (N.D. Cal. July 15, 2025)..... 10

Chanel, Inc. v. Doren,
No. 3:15-CV-1393-M (BF), 2016 WL 7444995 (N.D. Tex. Nov. 28, 2016), *R&R adopted*,
2016 WL 7468068 (N.D. Tex. Dec. 27, 2016) 25

Commonspirit Health v. Emerge Clinical Sols., LLC,
No. 3:22-CV-2750-L, 2022 WL 17903800 (N.D. Tex. Dec. 23, 2022) 22

Corp. Relocation, Inc. v. Martin,
No. 3:06-CV-232-L, 2006 WL 4101944 (N.D. Tex. Sept. 12, 2006) 25

Daniels Health Scis., L.L.C. v. Vascular Health Scis., L.L.C.,
710 F.3d 579 (5th Cir. 2013) 21

DHI Grp., Inc. v. Kent,
No. H-16-1670, 2017 WL 4837730 (S.D. Tex. Oct. 26, 2017) 16, 18

DISH Network L.L.C. v. Khalid,
No. CV H-19-4563, 2021 WL 765709 (S.D. Tex. Feb. 23, 2021) 23

Doe v. Tex. Christian Univ.,
601 F. Supp. 3d 78 (N.D. Tex. 2022) 21

Dyll v. Adams,
167 F.3d 945 (5th Cir. 1999) 17

TABLE OF AUTHORITIES
(continued)

Page(s)

Enargy Power Co. v. Xiaolong Wang
No. 13-11348-DJC, 2013 WL 6234625 (D. Mass. Dec. 3, 2013) 19

Facebook, Inc. v. Power Ventures, Inc., ("*Power Ventures I*"),
844 F.3d 1058 (9th Cir. 2016) 9, 10, 14, 20

Facebook, Inc. v. Power Ventures, Inc., ("*Power Ventures II*"),
252 F. Supp. 3d 765 (N.D. Cal. 2017), *aff'd*, 749 F. App'x 557 (9th Cir. 2019) 20

Fla. Atl. Univ. Bd. of Trs. v. Parsont,
465 F. Supp. 3d 1279 (S.D. Fla. 2020) 19, 22

Hoover v. Morales,
164 F.3d 221 (5th Cir. 1998) 7

Humana, Inc. v. Avram A. Jacobson, M.D., P.A.,
804 F.2d 1390 (5th Cir. 1986) 19

In re Complaint of Grand Famous Shipping Ltd.,
No. 4:18-CV-2046, 2024 WL 3620313 (S.D. Tex. Aug. 1, 2024) 17

Meta Platforms, Inc. v. Ates,
No. 22-CV-03918-TSH, 2023 WL 4035611 (N.D. Cal. May 1, 2023), *R&R adopted*, 2023 WL 4995717 (N.D. Cal. June 27, 2023) 20

Meta Platforms, Inc. v. Qibaa,
No. 25-CV-01678-TSH, 2025 WL 2496129 (N.D. Cal. Aug. 1, 2025) 21

MetroPCS v. Mohammad,
No. 3:16-CV-1946-BK, 2017 WL 2590108 (N.D. Tex. Apr. 2017), *R&R Adopted*,
No. 3:16-CV-1946-L, 2017 WL 2579040 (N.D. Tex. June 14, 2017) 11

Muhammad v. Green Tree Servicing, LLC,
No. 3:13-CV-2535-P, 2013 WL 12137723 (N.D. Tex. July 22, 2013) 7

Nat'l Presto Indus. Inc. v. Slate River Sys. Inc.,
No. 4:25-cv-00462, 2025 WL 2684327 (N.D. Tex. May 7, 2025) 24

Philips N. Am. LLC v. Image Tech. Consulting, LLC,
No. 3:22-CV-0147-B, 2024 WL 4876961 (N.D. Tex. Nov. 22, 2024) 11

R.R. Mgmt. Co., L.L.C. v. CFS La. Midstream Co.,
428 F.3d 214 (5th Cir. 2005) 15

Reliable Prop. Servs., LLC v. Cap. Growth Partners, LLC,
1 F. Supp. 3d 961 (D. Minn. 2014) 21

Rodriguez v. Google LLC,
772 F. Supp. 3d 1093 (N.D. Cal. 2025) 14

Ryanair DAC v. Booking Holdings Inc.,
No. CV 20-1191-WCB, 2024 WL 3732498 (D. Del. June 17, 2024) 9

Shurgard Storage Ctrs., Inc. v. Safeguard Self Storage, Inc.,
119 F. Supp. 2d 1121 (W.D. Wash. 2000) 12

TABLE OF AUTHORITIES
(continued)

Page(s)

State Analysis, Inc. v. Am. Fin. Servs. Assoc.,
621 F. Supp. 2d 309 (E.D. Va. 2009) 10

Sungdo ENG USA, Inc. v. Hyoungwon Inc.,
No. 1:23-CV-06025-TRJ, 2025 WL 2270146 (N.D. Ga. Mar. 19, 2025) 15

Sw. Airlines Co. v. BoardFirst, LLC,
No. 3:06-CV-0891-B, 2007 WL 4823761 (N.D. Tex. Sept. 12, 2007) ..... passim

Sw. Airlines Co. v. Kiwi.com, Inc.,
2021WL 4476799 (N.D. Tex. Sep. 30, 2021)..... 17, 21, 22

Totalcare Healthcare Servs., LLC v. TotalMD, LLC,
643 F. Supp. 3d 636 (N.D. Tex. 2022) 25

Valley v. Rapides Par. Sch. Bd.,
118 F.3d 1047 (5th Cir. 1997) 21

Statutes

18 U.S.C. § 1030(a) 8

18 U.S.C. § 1030(a)(4)..... 11

18 U.S.C. § 1030(e)(2)..... 11

18 U.S.C. §§ (c)(4)(A)(i)(I) 8

18 U.S.C. §§ 1030(a)(2)..... 8

47 U.S.C. § 222..... 22

Cal Civ. Code § 1798.150..... 22

Cal. Penal Code § (c)(7)..... 14

Cal. Penal Code § 502(c)(2)..... 13, 14

Cal. Penal Code § 502(c)(3)..... 14

Cal. Penal Code § 502(c)(7)..... 14

O.C.G.A. § 16-9-93(a) 15

O.C.G.A. § 16-9-93(a)(1) 15

O.C.G.A. § 16-9-93(a)(2) 15

Tex. Bus. & Com. Code § 521.052..... 22

Tex. Civ. Prac. & Rem. Code § 143.001(a)..... 12

Tex. Penal Code § 33.02(a)..... 12

Tex. Penal Code § 33.02(b-1) 12

I. INTRODUCTION

AT&T seeks a temporary restraining order and preliminary injunction to stop T-Mobile from taking customer data from secure, password-protected websites on AT&T's computer systems without AT&T's consent. AT&T has already told T-Mobile to stop. T-Mobile refused and instead actively circumvented security measures that AT&T put in place to block T-Mobile's unauthorized intrusions. AT&T needs an injunction to stop T-Mobile's unlawful conduct and prevent irreparable harm to AT&T's customers and its business, reputation, and goodwill.

* * *

Over the course of many years and billions of dollars in investments, AT&T has grown to serve over 119 million wireless customers nationwide. The trust of its customers is crucial to AT&T's success. To maintain that trust, AT&T prioritizes the security of customer data, taking comprehensive measures to ensure that it is handled responsibly and safely. AT&T also believes strongly that customers should be well-informed about the services they receive. To that end, AT&T provides customers with detailed data about their accounts, contracts, and billing through a password-protected, non-public customer websites.

T-Mobile also offers wireless services. But this case is not about competition for customers. It is about T-Mobile's deliberate, unauthorized, and deceptive intrusions into AT&T's computer systems to scrape AT&T customer data using its "T-Life App." On November 20, 2025, T-Mobile announced the beta launch of a new "AI-powered" tool called "Switch Made Easy" or "Easy Switch" ("SME") within the T-Life App, along with plans for a full launch on December 1, 2025. The SME scraping tool purports to formulate a competing wireless-service offer from T-Mobile for current AT&T (and Verizon) customers.

But to achieve its goal, SME relies on scraping password-protected websites hosted on AT&T servers for confidential customer information, including information that is not visible on AT&T customers' wireless bills or even through the customer portal. T-Mobile's scraper also operates without identification so as to appear as AT&T's own customers, in a blatant attempt to deceive AT&T's systems. This covert data harvesting is without authorization and in violation of AT&T's Terms of Use ("TOU") that govern the use of AT&T's websites.

T-Mobile has claimed its conduct is lawful because AT&T customers consent to T-Mobile obtaining their data when they use the T-Life App. But as a matter of law, customers alone cannot give consent to T-Mobile's unauthorized intrusions onto AT&T's systems. Only AT&T can authorize that and here, AT&T expressly informed T-Mobile that it does not consent.

AT&T attempted to avoid filing this lawsuit and motion. AT&T sent a cease-and-desist letter to T-Mobile on November 24, 2025, and on the same day, implemented computer security measures to block T-Mobile's unlawful scraping. But just a day later, on November 25, T-Mobile reengineered its SME scraping tool to further disguise it from detection. After AT&T implemented additional blocking measures, the next day, on November 26, T-Mobile again modified its SME scraping tool's disguise to evade detection.

After AT&T again blocked SME's access on November 26, T-Mobile removed its SME's scraping function for AT&T customers (but the tool still scrapes data of Verizon customers). At the same time, T-Mobile responded to AT&T's cease-and-desist letter, declaring that T-Mobile would not stop its misconduct and intended to release its SME scraping tool on December 1 as planned because, according to T-Mobile, it is "entirely lawful." Thus, AT&T has been left with no choice but to file this motion to maintain the status quo and enjoin T-Mobile's

intrusion into AT&T's systems, which violates the Computer Fraud and Abuse Act ("CFAA") and its state law counterparts, and breaches AT&T's TOU.

All four factors that courts consider strongly favor a temporary restraining order and preliminary injunction. First, AT&T is highly likely to succeed on the merits because T-Mobile's brazen scraping of password-protected customer data on AT&T's systems—despite AT&T's security measures and clear written notice to T-Mobile that it lacks authorization—violates federal and state laws, and it also breaches, and induces breaches of, AT&T's TOU. Second, T-Mobile's misconduct inflicts irreparable harm because it undermines AT&T's control over its servers and customer data and erodes its goodwill with its customers. Third, the injury to AT&T far outweighs any theoretical damage to T-Mobile, including because it is no burden for a defendant to be enjoined from illegal conduct. Fourth, the public interest demands immediate injunctive relief because T-Mobile's conduct is unlawful and harmful to customers.

II. FACTUAL BACKGROUND

A. AT&T's Protection Of Consumer Data And Terms Of Use

AT&T places a high value on the safety and security of its customers' data, continually investing in the best technology and practices to protect sensitive personal information, comply with privacy regulations, and prevent unauthorized access. AT&T employs industry-leading measures to ensure that customer data is handled securely, and these protections are especially robust for internet-facing systems, such as AT&T websites and password-protected customer portals. Ex. A, Abraham Decl. ¶ 9 (Appx004); Ex. B, Kia Decl. ¶ 6 (Appx026). AT&T also implements a range of advanced security measures to detect and block unauthorized access to AT&T's systems and shield against common web exploits. For example, AT&T has previously blocked bad actors who launch phishing attacks or attempt to use customer credentials to access

internal AT&T tools. Ex. A, Abraham Decl. ¶¶ 10–11 (Appx004).

AT&T also maintains a comprehensive TOU governing access to its public and non-public websites. AT&T's TOU applies to everyone accessing its websites—including T-Mobile—and includes many provisions designed to safeguard customer information and the integrity of AT&T's systems. Ex. B-1, AT&T's TOU § 1 (Appx032) ("by accessing or using our site in any way you are agreeing to comply with these Terms of Use"). AT&T's TOU prohibits any activity that (1) "uses any robot, spider, or other such programmatic or automatic device . . . to obtain information from the Site or otherwise monitor or copy any portion of the Site, products and/or services"; (2) "uses, downloads or otherwise copies any user information and/or usage information for any portion thereof, or transmit, provide or otherwise distribute . . . such information to any third party"; (3) "collects and uses any Content, including the use of any data mining, or similar data gathering or extraction methods." *Id.* § 14 (Appx035). The TOU further states that "[e]xamples of security violations include, without limitation, unauthorized access to or use of data or systems." *Id.* § 15 (Appx035–036).

AT&T's password protected, non-public websites being targeted by T-Mobile are subject to the TOU and provide customers with detailed data about their user accounts, contracts, wireless plans, billing, promotions, and subscriptions. Ex. A, Abraham Decl. ¶¶ 4–8 (Appx002–004); Ex. B, Kia Decl. ¶¶ 7–11 (Appx026–028). One way AT&T customers can access their account data is logging into a customer portal with a username and password, linked to their AT&T account online at https://signin.att.com/. Ex. A, Abraham Decl. ¶¶ 5–7 (Appx003).

B. T-Mobile's "Switch Made Easy" Relies On Bots Scraping AT&T's Websites

Like AT&T, T-Mobile offers wireless service. In early 2024, T-Mobile published a mobile phone application called the T-Life App, which has been installed over 90 million times

and can be installed on devices subscribed to AT&T services. On November 20, 2025, T-Mobile announced an "AI-powered" tool within the T-Life App called "Switch Made Easy" ("SME"), with a launch date of December 1, 2025. Ex. A-1, T-Mobile Press Release (Appx018–023).

According to T-Mobile, SME helps potential customers "identify and recommend the best plans for the customer, based on their current AT&T or Verizon account." *Id.* But to accomplish that goal, T-Mobile required the user to log in to their AT&T account through the T-Life App, upon which, the SME scraping tool—disguised to AT&T as the customer—harvests the customer's confidential data from password-protected AT&T websites hosted on AT&T's servers and sends that data back to T-Mobile's servers. Ex. A, Abraham Decl. ¶¶ 15–18 (Appx006–008). The SME scraping tool extracts over 100 categories of private information, including: billing and physical addresses, email address, billing and billing history, device and phone plan details, trade-in values, installment plans and payoffs, available upgrades and upgrade pathways, charges and disputes, number of lines on the account and details of lines (including for family members), usage details, and information about other services such as home internet. *Id.* ¶ 23 (Appx009). Much of this internal information goes far beyond the information that is visible on a user's AT&T wireless bill or customer portal. *Id.* ¶ 7 (Appx003).

C. AT&T's Detection Of T-Mobile's Scraping Tool and Pre-Litigation Response

Immediately after the November 20, 2025 release of the beta version of the SME scraping tool, AT&T detected that T-Mobile was scraping AT&T customer account data hosted on AT&T's servers in Dallas, Texas, Alpharetta, Georgia, and Fairfield, California. *Id.* ¶ 22 (Appx009). AT&T's investigation showed that T-Mobile designed SME to hide its unauthorized access to AT&T's systems. *Id.* ¶¶ 24–25 (Appx009–010). For example, when the SME scraping tool initially accesses ***AT&T's*** servers and issues requests to scrape data, it omits any

identification information associating itself with the T-Life App or T-Mobile. *Id.* ¶ 25 (Appx010). But when the SME scraping tool later sends scraped customer data to ***T-Mobile's*** servers, it identifies the response as associated with T-Mobile's T-Life App name, *i.e.*, "Origin-Application-Id=TLIFE." *Id.* ¶ 25 (Appx010). The only logical inference from the T-Mobile's selective self-identification is that it is attempting to hide its misconduct from AT&T.

On November 24, 2025, AT&T sent a cease-and-desist letter demanding that T-Mobile stop its unauthorized access of AT&T's systems. Ex. C-1, C&D Letter (Appx045). AT&T's letter was unequivocal that T-Mobile's use of SME to access AT&T's systems is unauthorized by AT&T and a breach of AT&T's TOU. *Id.* 3–4 (Appx047–048). On November 26, T-Mobile responded to AT&T's cease-and-desist letter and refused to end its SME scraping tool, claiming that "Easy Switch is entirely lawful" because "customers themselves . . . log into their own wireless account." Ex. C-2, Response to C&D Letter at 1–2 (Appx051–052).

AT&T also contacted Apple Inc. on November 24, with its concerns that the T-Life App, with the SME scraping tool, violates Apple's App Store Review Guidelines. Ex. C-3, Apple Notice of Complaint Email 5–7 (Appx058–060). In response, on November 28, T-Mobile made similar misstatements to Apple about the legality of SME and asserted that SME does not violate Apple's guidelines. Ex. C-3, Apple Notice of Complaint Email Thread 1 (Appx054).

Since November 24, AT&T has also been implementing security measures to block SME's unauthorized access to AT&T's systems, including by detecting behaviors associated with the SME scraping tool. Ex. A, Abraham Decl. ¶¶ 26–30 (Appx010–012). But only a day after AT&T rolled out its security measures on November 24, AT&T detected that T-Mobile had modified SME to further disguise itself to circumvent AT&T's security measures. *Id.* ¶¶ 31–32 (Appx012). After discovering T-Mobile's reengineered data scraper, on November 25, AT&T

implemented more security measures to prevent T-Mobile's unauthorized access to its systems. *Id*. ¶¶ 33–34 (Appx012–013). In response to AT&T's second set of measures, on November 26, T-Mobile once again modified the SME scraping tool to circumvent AT&T's protections. *Id*. ¶¶ 35–37 (Appx013). AT&T has since been forced to implement a ***third*** set of security measures to prevent T-Mobile's unauthorized scraping. *Id*. ¶ 38 (Appx013).

After this third set of measures, on the evening of November 26, T-Mobile updated SME to remove the scraping function; SME currently asks AT&T customers to upload a PDF of their bill or enter certain AT&T account information manually, rather than scraping AT&T websites (though it still appears to scrape Verizon's websites). *Id*. ¶ 39 (Appx013–014). T-Mobile's legal position, however, remains unchanged from its cease-and-desist response: fervently declaring that it intends to continue using SME to scrape AT&T's websites.

III. LEGAL STANDARD

The standard for a temporary restraining order and preliminary injunction is the same: a party must show "(1) a substantial likelihood of success on the merits; (2) a substantial threat that the movant will suffer irreparable injury if the injunction is denied; (3) the threatened injury outweighs any damage that the injunction might cause the defendant; and (4) the injunction will not disserve the public interest." *Hoover v. Morales*, 164 F.3d 221, 224 (5th Cir. 1998) (citations omitted) (preliminary injunction); *see also Muhammad v. Green Tree Servicing, LLC*, No. 3:13-CV-2535-P, 2013 WL 12137723, at *1 (N.D. Tex. July 22, 2013) (temporary restraining order).

IV. ARGUMENT

AT&T is entitled to immediate injunctive relief. T-Mobile's covert scraping of private customer data from AT&T's password-protected systems plainly violates the Computer Fraud and Abuse Act ("CFAA"), and its state law counterparts, Texas' Harmful Access by Computer

Act, California's Computer Data Access and Fraud Act, and Georgia's Computer Systems Protection Act. T-Mobile's bad acts also constitute a breach of contract (i.e., AT&T's TOU) and tortious interference with AT&T's contracts with its customers. T-Mobile's misconduct inflicts irreparable harm of the type consistently recognized in computer scraping cases. Finally, the balance of equities and public interest favor an injunction.

A. AT&T Is Likely to Succeed On Each Of Its Claims

1. Count I: Computer Fraud and Abuse Act, 18 U.S.C. § 1030(a)(2), (a)(4)

The CFAA "prohibits acts of computer trespass by unauthorized users." *Am. Airlines, Inc. v. Red Ventures LLC*, No. 4:22-CV-0044-P, 2022 WL 2790643, at *4 (N.D. Tex. July 15, 2022). T-Mobile's unauthorized access to AT&T's servers violates two CFAA provisions: (1) § 1030(a)(2) by accessing AT&T's servers "without authorization" to obtain information and (2) § 1030(a)(4) by accessing AT&T's servers "knowingly and with intent to defraud."

a. CFAA, Section 1030(a)(2)

T-Mobile's misconduct meets the elements of a § 1030(a)(2) claim, which requires that T-Mobile (1) intentionally accessed a computer, (2) without authorization, (3) and thereby obtained information (4) from a protected computer, and (5) caused a loss of at least $5,000 in a one-year period. *See* 18 U.S.C. §§ 1030(a)(2), (c)(4)(A)(i)(I).

First, T-Mobile "intentionally accessed" AT&T's servers. *See* 18 U.S.C. § 1030(a). The SME scraping tool works by harvesting customer data accessible only on password-protected sections of AT&T's website, hosted on AT&T's servers. Ex. A, Abraham Decl. ¶ 20 (Appx009). T-Mobile's acts are intentional, as proven by its repeated efforts to circumvent AT&T's measures to block SME's access and T-Mobile's express refusal to cease-and-desist.

Second, T-Mobile's access to AT&T's servers is "without authorization." AT&T never authorized T-Mobile's access through the SME scraping tool. Despite T-Mobile's assertions that the SME is "entirely lawful," AT&T's TOU expressly prohibits such conduct. Ex. C-2, Response to C&D Letter 1 (Appx051); Ex. B-1, TOU at §§ 14–15 (Appx035–036). To the extent T-Mobile claims ignorance, AT&T's November 24 cease-and-desist letter leaves no room for T-Mobile to dispute that it lacked authorization to access AT&T's servers. Ex. C-1, C&D Letter 1 (Appx045) ("AT&T is writing to demand that T-Mobile immediately stop its unlawful attempts to access and misuse AT&T customers' private information.").

T-Mobile cannot sidestep its missing authorization by contending that it obtained customers' consent to scrape AT&T's systems because "customers themselves . . . log into their own wireless account." Ex. C-2, Response to C&D Letter 2 (Appx052). Courts across the country have uniformly held that "authorization" under the CFAA cannot be from the customer alone. Rather, "authorization" must come from ***both*** the owner of the "protected computer" or servers—here AT&T—***and*** the customer. *E.g.*, *Facebook, Inc. v. Power Ventures, Inc.*, ("*Power Ventures I*"), 844 F.3d 1058, 1067–68 (9th Cir. 2016); *ACI Payments, Inc. v. Conservice, LLC*, No. 121CV00084RJSCMR, 2022 WL 622214, at *11 (D. Utah Mar. 3, 2022) (rejecting defendant's argument that it has been authorized by Speedway's customers to access their Speedway accounts where such access violated Speedway's terms of use, and defendant "was put on notice of this violation through multiple cease-and-desist letters"); *Ryanair DAC v. Booking Holdings Inc.*, No. CV 20-1191-WCB, 2024 WL 3732498, at *10 (D. Del. June 17, 2024) (explaining that defendants' access to "the password-protected portion of the myRyanair website after Ryanair issued cease-and-desist letters" is "without authorization" under the CFAA); *CDK Glob., LLC v. Tekion Corp.*, No. 25-CV-01394-JSC, 2025 WL 1939951, at *6

(N.D. Cal. July 15, 2025) (defendant lacked authorization under the CFAA where it relied on customer credentials to extract information from plaintiff's password-protected databases and the defendant had been informed that those customers were prohibited "from sharing their . . . access with unauthorized third parties"); *State Analysis, Inc. v. Am. Fin. Servs. Assoc.*, 621 F. Supp. 2d 309, 316 (E.D. Va. 2009) (holding that defendant lacked authorization under the CFAA, while rejecting defendant's argument it was granted authorization by users of plaintiff's website).

Power Ventures I is particularly apposite. In that case, the defendant scraped password-protected user pages of the Facebook website. 844 F.3d at 1068. Just like AT&T, Facebook responded with a cease-and-desist letter and technical barriers to access. *Id.* The Ninth Circuit held that the defendant's efforts to access Facebook's computers were "without authorization" because "[t]he consent that [defendant] had received from Facebook users was not sufficient to grant continuing authorization to access Facebook's computers after Facebook's express revocation of permission." *Id*. The same is true here: even if customers allegedly consent by logging into their AT&T accounts, T-Mobile's lacks consent from AT&T and, thus its intrusions and scraping are "without authorization" under the CFAA.

Third, T-Mobile "obtained" vast amounts of "information" from AT&T's servers. The SME scraping tool extracts over 100 categories of customer data, including: billing and physical addresses, email address, billing and billing history, device and phone plan details, trade-in values, installment plans and payoffs, available upgrades and upgrade pathways, charges and disputes, number of lines on the account and details of lines (including for family members), usage details, and information about other services such as home internet. Ex. A, Abraham Decl. ¶ 23 (Appx009). This scraped data includes far more data that is visible or available to a customer through their AT&T wireless bill or its account portal. *Id.* ¶ 7 (Appx003). And

AT&T's investigation of network traffic shows that T-Mobile has transmitted all this data to T-Mobile's own servers, over which AT&T has no control. *Id.* ¶ 25 (Appx010).

Fourth, AT&T's servers are "protected computers" under the CFAA, which defines a "protected computer" to include any computer "used in or affecting interstate or foreign commerce." 18 U.S.C. § 1030(e)(2). AT&T's servers are connected to the internet, so they are necessarily used in and affect interstate commerce. *See MetroPCS v. Mohammad*, No. 3:16-CV-1946-BK, 2017 WL 2590108, at *4 (N.D. Tex. Apr. 2017), *R&R Adopted*, No. 3:16-CV-1946-L, 2017 WL 2579040 (N.D. Tex. June 14, 2017).

Fifth, AT&T has suffered a "loss" of more than $5,000 during a one-year period as a direct result of T-Mobile's unauthorized access, including over 1,000 man-hours of engineer time since November 20, 2025, investigating and responding to T-Mobile's SME scraping tool. Ex. A, Abraham Decl. ¶ 42 (Appx015). These costs of "responding to an offense" and "internal investigation" qualify as a "loss" under the CFAA. *See Philips N. Am. LLC v. Image Tech. Consulting, LLC*, No. 3:22-CV-0147-B, 2024 WL 4876961, at *9 (N.D. Tex. Nov. 22, 2024) (granting summary judgment in favor of plaintiff's CFAA claim).

b. CFAA, Section 1030(a)(4)

A § 1030(a)(4) claim requires proof of the same elements as § 1030(a)(2) but adds that the access must be made knowingly and with an intent to defraud. *See* 18 U.S.C. § 1030(a)(4). The CFAA's concept of "defraud" is broad, "simply mean[ing] wrongdoing and does not require proof of common law fraud." *Barnstormers, Inc. v. Wing Walkers, LLC*, No. EP-10-CV-261-KC, 2011 WL 1671641, at *10 (W.D. Tex. May 3, 2011).

Here, the very design of the SME scraping tool shows T-Mobile's intent to defraud by disguising its intrusions as legitimate customer traffic. Under common industry practice,

T-Mobile's user agent string—a piece of information sent by a requester, such as a web browser, to identify itself to a server—should have identified its origin as the T-Life App. But when the SME scraping tool initially accesses ***AT&T's*** servers, it omits any identifier that can be linked to T-Mobile. Ex. A, Abraham Decl. ¶ 24 (Appx009–010). Yet, when the SME tool later sends back messages (with scraped AT&T data) to T-Mobile's ***own*** servers, the SME follows industry practice by including in its user agent string, "Origin-Application-Id=TLIFE," which clearly ties the sender to T-Mobile's T-Life App. *Id*. ¶ 25 (Appx010). What's more, since November 24, T-Mobile has twice reengineered its SME scraping tool to modify its disguise and evade detection in response to AT&T's new security measures. *Id*. ¶ 31, 37 (Appx012–013). T-Mobile's intentional obfuscation of the scraping tool's identity is a knowing action made with the purpose of defrauding AT&T. *See Shurgard Storage Ctrs., Inc. v. Safeguard Self Storage, Inc.*, 119 F. Supp. 2d 1121, 1126 (W.D. Wash. 2000) (finding § 1030(a)(4) claim viable where "the defendant participated in dishonest methods to obtain the plaintiff's secret information").

2. Count II: Tex. Comp. Crimes, Tex. Penal Code § 33.02, Civil Code § 143.001

T-Mobile's conduct also violates Texas's Harmful Access by Computer Act, which prohibits T-Mobile from "knowingly access[ing] a computer, computer network, or computer system without the effective consent of the owner." Tex. Penal Code § 33.02(a); Tex. Civ. Prac. & Rem. Code § 143.001(a). Texas also penalizes T-Mobile from committing such an offense "with the intent to defraud or harm another or alter, damage, or delete property." Tex. Penal Code § 33.02(b-1). Further, access in violation of a website's terms of use constitutes access without effective consent. *See Sw. Airlines Co. v. BoardFirst, LLC*, No. 3:06-CV-0891-B, 2007 WL 4823761, at *16 (N.D. Tex. Sept. 12, 2007) (holding that because defendant's use of

Southwest's site "falls squarely within [the terms of use] prohibitions," "the undisputed summary judgment evidence shows" defendant's access was without effective consent).

T-Mobile knowingly, and with the intent to defraud and harm AT&T, accessed AT&T's servers. T-Mobile purposely designed its SME scraping tool to access AT&T's servers and take password-protected customer information, in violation of AT&T's TOU. *See* Ex. B-1, TOU § 14 (Appx035); Ex. A, Abraham Decl. ¶ 24 (Appx009–010); *see also* Section A.I–II. Just as in *BoardFirst*, T-Mobile's blatant violation of AT&T's publicly accessible TOU establishes a lack of effective consent. *See BoardFirst*, 2007 WL 4823761, at *16; *see* Ex. B-1, TOU § 14 (Appx035); Ex. A, Abraham Decl. ¶ 9 (Appx004).

Further, T-Mobile's subsequent evasion confirms its guilty intent: T-Mobile knows it does not have AT&T's consent to access the data, so T-Mobile further disguised its scraping tool twice to circumvent AT&T's enhanced security measures. Ex. A, Abraham Decl. ¶ 31, 37 (Appx012–013). T-Mobile's blatant disregard of the TOU, cease-and-desist letter, and security measures all demonstrate knowing, intentional, and fraudulent access to AT&T's Dallas-based servers. Ex. C-2, Response to C&D Letter 1-2 (Appx051–052).

3. Count III: Cal. Computer Data Access and Fraud Act, Cal. Penal Code § 502

Because some of AT&T's attacked servers are in California, T-Mobile's conduct also violates the California Computer Data Access and Fraud Act , which "is broader than CFAA in many respects." *Biden v. Ziegler*, 737 F. Supp. 3d 958, 975 (C.D. Cal. 2024). T-Mobile's actions violate at least three provisions of the statute: (1) "[k]nowingly accesses and without permission takes, copies, or makes use of any data from a computer, computer system, or computer network, or takes or copies any supporting documentation, whether existing or residing internal or external to a computer, computer system, or computer network," Cal. Penal Code § 502(c)(2); (2) "[k]nowingly and without permission uses or causes to be used computer

services," *id.* § 502(c)(3); and (3) "[k]nowingly and without permission accesses or causes to be accessed any computer, computer system, or computer network," *id.* § 502(c)(7).

T-Mobile's conduct violates each prong of these three provisions. First, T-Mobile "knowingly accesse[d]" AT&T's servers by deploying its SME scraping tool with knowledge and intent that it would scrape customer data from AT&T servers, for the reasons detailed above for the Texas counterpart statute. Second, T-Mobile's access was "without permission" as even after receiving AT&T's November 24 cease-and-desist letter, T-Mobile affirmatively stated it would continue its scraping activities and continued to do so. Ex. C-2, Response to C&D Letter 2 (Appx052); *see Power Ventures I*, 844 F.3d at 1069 (affirming violation where defendant scraped after it "knew that it no longer had permission to access" from plaintiff's cease-and-desist letter). Third, T-Mobile's conduct included "cop[ying]" and "mak[ing] use of" data acquired through its scraping by transmitting that data back to T-Mobile's own servers, § 502(c)(2), and "us[ing]" and "access[ing]" AT&T's "computer services" and "system[s]" by intruding on its servers to obtain such data, Cal. Penal Code §§ 502(c)(3), (c)(7). Fourth, AT&T suffered "damage or loss by reason of" T-Mobile's violations, including costs of having to investigate and respond to T-Mobile's trespass, including implementing additional technical barriers to prevent T-Mobile's continued access. Ex. A, Abraham Decl. ¶¶ 26–38 (Appx010–013); *see Rodriguez v. Google LLC*, 772 F. Supp. 3d 1093, 1109 (N.D. Cal. 2025).

4. Count IV: Georgia Computer Systems Protections Act, O.C.G.A. § 16-9-93

T-Mobile's conduct also violates the Georgia Computer Systems Protections Act, which applies here because some of AT&T's attacked servers are in Georgia. Under the statute, "[a]ny person who uses a computer or computer network with knowledge that such use is without authority and with the intention of: (1) taking or appropriating any property of another, whether

or not with the intention of depriving the owner of possession; [or] (2) obtaining property by any deceitful means." O.C.G.A. § 16-9-93(a).

T-Mobile's misconduct satisfies each element. First, T-Mobile is "us[ing] a computer or computer network with knowledge that such use is without authority." *See id.* T-Mobile continued to deploy its SME scraping tool after AT&T sent its cease-and-desist letter, including reengineering the tool twice to circumvent AT&T's security measures. Ex. A, Abraham Decl. ¶¶ 31, 37 (Appx012–013). Second, T-Mobile's data scraping appropriated AT&T's property in the form of AT&T customer account data. *See* O.C.G.A. § 16-9-93(a)(1); *Sungdo ENG USA, Inc. v. Hyoungwon Inc.*, No. 1:23-CV-06025-TRJ, 2025 WL 2270146, at *2 (N.D. Ga. Mar. 19, 2025) (finding a violation where the defendant appropriated plaintiff's information after receiving demand to cease). Third, T-Mobile obtained AT&T's property with "deceitful means" by disguising the SME scraping tool to avoid affiliation with T-Mobile. *See id.* § 16-9-93(a)(2).

5. Count V: Breach of Contract

Texas law applies to the TOU. To establish a breach of contract claim under Texas law, "a plaintiff must prove (1) the existence of a valid contract; (2) the plaintiff's performance or tendered performance; (3) the defendant's breach of the agreement; and (4) the plaintiff's resulting damages." *BoardFirst,* 2007 WL 4823761, at *4. Here, all four elements are met.

First, there is a valid existing contract between AT&T and T-Mobile because T-Mobile assented to the TOU, a browsewrap agreement on AT&T's website. Courts in this District have held that whether a website's terms of use is a binding contract turns on whether a website user has assented to those terms. *See id*. at *5. Assent need not be express—it may be manifested indirectly through one's conduct. *See id*. at *4 (citing *R.R. Mgmt. Co., L.L.C. v. CFS La. Midstream Co.*, 428 F.3d 214, 222 (5th Cir. 2005)). A website user assents to a browsewrap

agreement by simply using the website, provided the plaintiff shows that "the user had actual or constructive knowledge of a sites terms and conditions." *Id.*; *see Andra Grp., LP v. BareWeb, Inc.*, No. 4:17-CV-00815, 2018 WL 2848985, at *9 (E.D. Tex. June 11, 2018).

T-Mobile had both actual and constructive knowledge of the TOU, making the TOU a valid contract between T-Mobile and AT&T. T-Mobile acquired actual knowledge of AT&T's TOU no later than when it received the November 24, 2025 cease-and-desist letter from AT&T expressly stating that Defendant's actions violated its TOU. Ex. C-1, C&D Letter 2 (Appx046); *see BoardFirst*, 2007 WL 4823761, at *7 (holding that continued site use after receiving a cease-and-desist letter was sufficient to establish actual knowledge and therefore assent to the terms). Even before receiving AT&T's letter, T-Mobile had constructive knowledge because T-Mobile has its ***own*** browsewrap terms of use for T-Mobile's own websites and T-Mobile's terms contain similar prohibitions against data scraping—making any argument that T-Mobile lacked knowledge of the TOU wholly implausible. *See DHI Grp., Inc. v. Kent*, No. H-16-1670, 2017 WL 4837730, at *4 (S.D. Tex. Oct. 26, 2017) ("allegations that DHI knew or should have known about the browsewrap agreement because it uses a similar agreement on its own site are sufficient to state a plausible claim for relief"); Ex. C-4, T-Mobile TOU 2 (Appx063).

Second, AT&T performed its obligations under the TOU by, among other things, making the public portions of AT&T websites available to T-Mobile subject to the defined terms.

Third, T-Mobile breached multiple provisions of the TOU by scraping confidential AT&T customer data from password-protected AT&T websites. T-Mobile breached the TOU's prohibitions against any activity that: (1) "uses any robot, spider, or other such programmatic or automatic device . . . to obtain information from the Site"; (2) "uses, downloads or otherwise copies any information and/or usage information for any portion thereof, or transmit, provide or

otherwise distribute . . . such information to any third party"; and (3) "collects and uses any Content, including the use of any data mining, or similar data gathering or extraction methods." Ex. B-1, TOU § 14 (Appx035).

Fourth, AT&T has suffered damage from T-Mobile's breach of the TOU, including its investigation and mitigation costs in implementing multiple rounds of security measures. Ex. A, Abraham Decl. ¶¶ 26–38 (Appx010–013); *see In re Complaint of Grand Famous Shipping Ltd.*, No. 4:18-CV-2046, 2024 WL 3620313, at *41 (S.D. Tex. Aug. 1, 2024). AT&T has also suffered reputational damage and loss of customer goodwill, as detailed further in Section IV.B relating to irreparable harm. *See Sw. Airlines Co. v. Kiwi.com, Inc.*, 2021WL 4476799, at *4 (N.D. Tex. Sep. 30, 2021). Although damage to reputation or goodwill is difficult to quantify, Texas courts do not prevent recovery for breach of contract merely because of "uncertainty as to their ***amount***" of damages resulting from a breach. *See BoardFirst*, 2007 WL 4823761, at *10 (emphasis original; citing *Dyll v. Adams*, 167 F.3d 945, 947 (5th Cir. 1999)).

6. Count VI: Tortious Interference With Contract

Under Texas law, the elements of a claim for tortious interference with contract are (1) an existing contract subject to interference, (2) a willful and intentional act of interference with the contract, (3) that proximately caused the plaintiffs injury, and (4) actual damages or loss. *Amigo Broad., LP v. Spanish Broad. Sys., Inc.*, 521 F.3d 472, 489 (5th Cir. 2008). Here, T-Mobile has tortiously interfered with the TOU, which is a contract between AT&T and its customers.

First, AT&T has existing contractual relationships with its customers, who register for an account on AT&T's portal and, in doing so, must affirmatively accept AT&T's TOU via a clickwrap agreement. Ex. A, Abraham Decl. ¶ 4 (Appx002); *see Am. Eyewear, Inc., v. Peeper's Sunglasses & Acc., Inc.,* 106 F. Supp. 2d 895, 904 n.15 (N.D. Tex. 2000).

Second, through its SME scraping tool, T-Mobile interfered with these contractual relationships by inducing AT&T's customers to grant the SME scraping tool access to their confidential customer account data on AT&T's secure websites, in breach of § 14 of the TOU. Acts of interference are intentional or willful where the interfering party knew or reasonably should have known of the existence of the contract between the plaintiff and a third party. *See Amigo Broad*, 521 F.3d at 490. Here, T-Mobile had actual knowledge of the TOU that applies between AT&T and anyone who accesses AT&T websites (including AT&T's customers) by no later than November 24, 2025, when T-Mobile received the cease-and-desist letter from AT&T. Despite this actual knowledge, T-Mobile continued to induce customers to allow the SME to scrape AT&T's website and customer account data in ways that violate the TOU.

Even before AT&T's letter, T-Mobile had constructive knowledge that the TOU applies between AT&T and its customers who use AT&T's website. The TOU is publicly available online. Ex. B-1, TOU (Appx032–037), https://www.att.com/legal/terms.attWebsiteTermsOfUse.html. AT&T provides notice that use of its websites is conditioned upon compliance with its TOU by attaching a hyperlink at the bottom of the page, as is standard practice for commercial websites. *Id*. Furthermore, T-Mobile is a sophisticated party who has its own terms of use that similarly prohibits scraping of its own websites, a fact that courts have found sufficient to find constructive knowledge of plaintiff's similar terms. *See DHI Grp.*, 2017 WL 4837730, at *4.

As established above for breach of contract (Section IV.A.5), T-Mobile's inducement of AT&T's customers has actually and proximately caused AT&T many forms of damages, which also satisfy the damages requirement for a tortious interference claim.

B. AT&T Has And Will Suffer Immediate, Irreparable Harm

To satisfy the irreparable harm standard, a "plaintiff need show only a significant threat of injury from the impending action, that the injury is imminent, and that money damages would not fully repair the harm." *Humana, Inc. v. Avram A. Jacobson, M.D., P.A.*, 804 F.2d 1390, 1394 (5th Cir. 1986). A "finding of irreparable harm is appropriate even where economic rights are involved when the nature of those rights makes establishment of the dollar value of the loss . . . especially difficult or speculative." *Allied Mktg. Grp., Inc. v. CDL Mktg., Inc.*, 878 F.2d 806, 810 n.1 (5th Cir. 1989). Here, T-Mobile's SME scraping tool will irreparably harm AT&T by: (1) interfering with AT&T's control of its own computer systems and data; and (2) damaging AT&T's goodwill and reputation with its customers. Each of these losses have been recognized as irreparable harms by courts in similar scraping cases that also involved claims under the CFAA and its state counterparts, or contract-based claims.

First, under the CFAA and its state counterparts, "federal courts around the country agree that the interference with an entity's control of its computer systems constitutes irreparable injury" and have thus enjoined such interference from occurring, even if that interference was already underway. *Fla. Atl. Univ. Bd. of Trs. v. Parsont*, 465 F. Supp. 3d 1279, 1296–97 (S.D. Fla. 2020) (collecting cases, and granting injunction because otherwise, if "the Defendants to continue accessing [plaintiff's] servers, [plaintiff] could never be certain that it was adequately protecting its students' proprietary information); *Enargy Power Co. v. Xiaolong Wang*, No. 13-11348-DJC, 2013 WL 6234625, at *10 (D. Mass. Dec. 3, 2013) ("[P]revent[ing] Enargy from enjoying the uninterrupted use of its [server] . . . constitutes irreparable harm.").

The *Power Ventures* decisions are illustrative: there, the defendant, who operated its own social networking site that competed with defendant Facebook, "took, copied, or made use of

data from the Facebook website" through the existing Facebook users' accounts. *Power Ventures I*, 844 F.3d at 1067–68. After the Ninth Circuit affirmed that defendant had violated the CFAA and its California counterpart, the district court entered a permanent injunction, finding irreparable harm because the defendant "in accessing Facebook's computers without authorization . . . interfered with Facebook's right to control access to its own computers and have acquired data to which Defendants have no lawful right." *Facebook, Inc. v. Power Ventures, Inc.,* ("*Power Ventures II*"), 252 F. Supp. 3d 765, 782 (N.D. Cal. 2017), *aff'd*, 749 F. App'x 557 (9th Cir. 2019). Notably, the court granted the injunction after the defendant's scraping conduct had already begun, finding this fact supported that "Facebook will suffer irreparable harm again" because—just like T-Mobile here—the defendants "frequently exhibited bad faith conduct that indicates that they will not easily be deterred from attempting to access Facebook's servers without authorization in violation of the CFAA." *Id*.

Similarly, in this District, Judge Boyle in *BoardFirst* found irreparable harm resulting from a breach of contract, where the defendant—in disregard of Southwest's own TOU for its websites and cease-and-desist letter—accessed and obtained information from Southwest's websites, which were protected by login credentials of Southwest customers. 2007 WL 4823761, at *17–18; *see also Meta Platforms, Inc. v. Ates*, No. 22-CV-03918-TSH, 2023 WL 4035611, at *8–9 (N.D. Cal. May 1, 2023), *R&R adopted*, 2023 WL 4995717 (N.D. Cal. June 27, 2023) (granting injunction against defendant who collected information in violation of Instagram's Terms of Use because his "'scraping of [] data and unauthorized use of Plaintiff's platform' gives rise to irreparable injury").

Here, T-Mobile's unauthorized misconduct has interfered with AT&T's control over its servers and the private customer data stored on those servers. Moreover, this interference will

only escalate. T-Mobile has shown that it will persistently seek to circumvent new safeguards that AT&T implements. And T-Mobile has refused AT&T's cease-and-desist demands, declaring that its SME scraping tool is lawful and will be fully released December 1 as planned. Ex. C-2, Response to C&D Letter 1–2 (Appx051–052). Accordingly, AT&T's loss of control over the integrity of its computer systems and its customer data constitutes irreparable harm under its statutory computer fraud and contract claims.

Second and independently, courts "routinely find that reputational harm can constitute irreparable injury . . . [because] [i]njury to reputation or goodwill is not easily measurable in monetary terms." *Doe v. Tex. Christian Univ.*, 601 F. Supp. 3d 78, 94–95 (N.D. Tex. 2022) (citing *Daniels Health Scis., L.L.C. v. Vascular Health Scis., L.L.C.*, 710 F.3d 579, 582 (5th Cir. 2013); *Valley v. Rapides Par. Sch. Bd.*, 118 F.3d 1047, 1056 (5th Cir. 1997)). In comparable cases involving CFAA and breach of contract claims, this District and others have recognized that unauthorized access to protected customer information or websites constitutes irreparable harm because such "activities are damaging its reputation and goodwill and these damages cannot be quantified." *Kiwi.com*, 2021 WL 4476799, at *6 (citations omitted); *Reliable Prop. Servs., LLC v. Cap. Growth Partners, LLC*, 1 F. Supp. 3d 961, 965 (D. Minn. 2014) (granting preliminary injunction and finding irreparable harm because defendant's unlawful taking of data about plaintiff's customers was "highly likely to damage [the plaintiff's] goodwill and its relationships with its customers"); *Meta Platforms, Inc. v. Qibaa*, No. 25-CV-01678-TSH, 2025 WL 2496129, at *9 (N.D. Cal. Aug. 1, 2025) (granting injunction where "Meta has suffered—and continues to suffer—irreparable harm to its reputation and goodwill as a result of Defendant's unauthorized access and use of Meta's platform that monetary damages cannot rectify"). In *Kiwi.com*, Judge Brown in this District enjoined the defendant from scraping

information from Southwest's website because it breached Southwest's websites' terms and conditions, which "caused Southwest to suffer damages . . . to its reputation and loss of goodwill from customer complaints and increased customer service burdens." 2021 WL 4476799, at *6.

Here, T-Mobile's SME scraping tool creates irreparable harm to AT&T's goodwill and reputation because of the immediate risk to the private data customers entrusted to AT&T. AT&T is entitled to—and indeed *required* to—control access to the private customer data stored on its servers because it has obligations, including under state and federal statutes (e.g., Tex. Bus. & Com. Code § 521.052, Cal Civ. Code § 1798.150, and 47 U.S.C. § 222), to securely maintain the consumer information it collects. Once SME sends scraped data to T-Mobile, AT&T has no control over how T-Mobile then stores and uses that extracted data. This exposes the sensitive customer data to third-party cyberattacks on T-Mobile's network, for which AT&T's customers may blame AT&T as the original and trusted collector of that data.

Moreover, AT&T has no way to prevent T-Mobile from misusing the exfiltrated customer information, whether for unwanted T-Mobile advertisement, sale to third-party marketers, or unauthorized publication. Ex. A, Abraham Decl. ¶ 41 (Appx014). Indeed, T-Mobile's Privacy Policy expressly permits the company to share data "to advertise and market products and services from T-Mobile and other companies," confirming the irreparable harm to AT&T. Ex. C-5, T-Mobile Privacy Policy 3 (Appx074); s*ee Commonspirit Health v. Emerge Clinical Sols., LLC*, No. 3:22-CV-2750-L, 2022 WL 17903800, at *2 (N.D. Tex. Dec. 23, 2022) (finding irreparable harm where defendant impermissibly held sensitive patient information collected by plaintiff); *Fla. Atl. Univ.*, 465 F. Supp. 3d at 1297 (finding unauthorized access to a university's email servers an irreparable injury because the university "could never be certain that it was adequately protecting its students' proprietary information").

AT&T's goodwill with customers is also put at risk by the security measures AT&T has been forced to implement since November 24 to block access by T-Mobile's SME scraping tool. In particular, given T-Mobile's continual efforts to mask its intrusions, the security measures AT&T has employed run the risk of "false positives"—misidentifying permissible activity by its actual customers as unauthorized T-Mobile intrusions, and then blocking those customers from being able to access their own accounts. Ex. A, Abraham Decl. ¶ 40 (Appx014). Any unintended blocking by AT&T damages its goodwill with those customers.

Further, handling the increased volume in requests created by T-Mobile's unauthorized intrusions impacts the processing capacity of AT&T servers. *Id*. ¶ 43 (Appx015). Not only does this place additional stress on AT&T's servers, potentially increasing costs and expenditure of resources, but it also hampers the user experience for legitimate customers because they will be competing for the same network resources as the SME scraping tool. *See Id.* This risk is particularly acute during AT&T's peak holiday sales season in December, when its systems are already experiencing high demand. *Id*.; Ex. B, Kia Decl. ¶ 13 (Appx029).

C. The Balance Of Equities Favors Granting Immediate Injunctive Relief

In weighing the balance of equities, no burden is imposed on a defendant by an injunction to refrain from further violating the law. *DISH Network L.L.C. v. Khalid*, No. CV H-19-4563, 2021 WL 765709, at *8 (S.D. Tex. Feb. 23, 2021) ("following the law is not a cognizable hardship in an injunction interest-balancing analysis"*)*; *Atl. Recording Corp. v. Anderson*, No. CIVA H-06-3578, 2008 WL 2316551, at *10 (S.D. Tex. Mar. 12, 2008) ("No burden is imposed on Defendant by an injunction to refrain from further infringements because he is merely required to comply with the law.").

As detailed above, T-Mobile's SME scraping tool violates multiple federal and Texas laws. AT&T simply seeks to stop T-Mobile's unlawful actions. T-Mobile therefore faces no legitimate, cognizable hardship should it be prevented from deploying the SME scraping tool on AT&T's password-protected websites. As a result, whatever efforts and resources T-Mobile claims to have expended in developing the SME scraping tool are irrelevant. As courts recognize, a defendant's interest in misusing plaintiff's website cannot outweigh the plaintiff's interest in protecting its website and goodwill. *See BoardFirst*, 2007 WL 4823761, at *18.

Even if T-Mobile had a legitimate interest in scraping private AT&T websites and customer data—and it does not—any hardship in ceasing that activity is minimal. Since the evening of November 26, T-Mobile has modified SME to end its scraping function, meaning it is no longer currently scraping AT&T customer data; SME instead currently asks AT&T customers to upload a PDF of their bill or enter account information manually. Ex. A, Abraham Decl. ¶ 39 (Appx013–014). Thus, at this time, granting this motion enjoining T-Mobile from using the SME scraping tool on AT&T's websites simply preserves the status quo, which favors entering preliminary injunctive relief and prohibiting T-Mobile from restarting and reusing the unlawful SME scraping tool in the future. *See Nat'l Presto Indus. Inc. v. Slate River Sys. Inc.*, No. 4:25-cv-00462, 2025 WL 2684327, at *2-3 (N.D. Tex. May 7, 2025) (finding balance favors plaintiff because status quo preserved by prohibition on defendant taking future, contemplated action).

D. The Public Interest Favors Granting Immediate Injunctive Relief

The public interest also favors enjoining T-Mobile's illicit SME scraping tool. Preventing illegal conduct is plainly in the public interest. *Chanel, Inc. v. Doren*, No. 3:15-CV-1393-M (BF), 2016 WL 7444995, at *7 (N.D. Tex. Nov. 28, 2016) ("the public interest would not be disserved by the issuance of a permanent injunction [which] prevent[s] . . . Defendants

from engaging in illegal conduct."), *R&R adopted*, 2016 WL 7468068 (N.D. Tex. Dec. 27, 2016). Similarly, the "public interest is served whenever state and federal laws are enforced." *Totalcare Healthcare Servs., LLC v. TotalMD, LLC*, 643 F. Supp. 3d 636, 650 (N.D. Tex. 2022). In addition, the public has an interest in the enforcement of contractual obligations. *Corp. Relocation, Inc. v. Martin*, No. 3:06-CV-232-L, 2006 WL 4101944, at *18 (N.D. Tex. Sept. 12, 2006) ("The public also has an interest in knowing and understanding that persons who breach their agreements may not profit or otherwise benefit from such conduct.").

All of these factors are present here. As explained throughout this motion, T-Mobile's operation of the SME scraping tool is illegal, violates federal and state laws, and breaches AT&T's TOU. The public interest therefore supports enjoining T-Mobile's wrongful conduct.

V. CONCLUSION

T-Mobile's unauthorized scraping of AT&T's systems violate several federal and state laws, while causing AT&T and its customers to suffer irreparable injuries. Judicial intervention is necessary to bring T-Mobile's harmful and unlawful activities to a halt. AT&T requests the Court to issue a temporary restraining order and preliminary injunction enjoining T-Mobile from any further unauthorized scraping of customer data from AT&T's websites.

Dated: November 30, 2025

O'MELVENY & MYERS LLP

By: /s/ *Timothy S. Durst*

TIMOTHY S. DURST (TX #00786924)
tdurst@omm.com
SID MODY (TX #24072791)
smody@omm.com
O'MELVENY & MYERS LLP
2801 North Harwood Street, Suite 1600
Dallas, TX 75201
Telephone: +1 972 360 1900

RANDALL W. EDWARDS (*pro hac vice* pending)
redwards@omm.com
MARK LIANG (*pro hac vice* pending)
mliang@omm.com
O'MELVENY & MYERS LLP
Two Embarcadero Center, 28th Floor
San Francisco, California 94111-3823
Telephone: +1 415 984 8700

REEMA SHAH (*pro hac vice* pending)
rshah@omm.com
O'MELVENY & MYERS LLP
1301 Avenue of the Americas 17th FL
New York, NY 10019-6022
Telephone: +1 212 326 2000

Attorneys for Plaintiffs AT&T SERVICES, INC. and AT&T MOBILITY LLC

CERTIFICATE OF SERVICE

I hereby certify that on November 30, 2025, a copy of the foregoing was served electronically via the CM/ECF to any parties that have appeared and by email to the lawyers noted below who have informed me they represent T-Mobile US, Inc. in this litigation.

/s/ Timothy S. Durst

SERVICE LIST

Hallie B. Levin
WILMERHALE
7 World Trade Center
250 Greenwich Street
New York, NY 10007
Hallie.Levin@wilmerhale.com

Ari Holtzblatt
WILMERHALE
2100 Pennsylvania Avenue NW
Washington, DC 20037
Ari.Holtzblatt@wilmerhale.com

Andreas Correa
Jared Eisenberg
LYNN PINKER HURST & SCHWEGMANN
2100 Ross Avenue, Suite 2700
Dallas, TX 75201
acorrea@lynnllp.com
jeisenberg@lynnllp.com