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

AT&T SERVICES, INC., and AT&T MOBILITY LLC	§	
Plaintiffs,	§	C.A. No. _____
v.	§	**JURY TRIAL DEMANDED**
T-MOBILE US INC.,	§	
Defendant.	§	

COMPLAINT AND REQUEST FOR INJUNCTIVE RELIEF

Plaintiffs AT&T Services, Inc. and AT&T Mobility LLC (collectively, "AT&T") file this Complaint and Request for Injunctive Relief against Defendant T-Mobile US Inc. ("T-Mobile")[1] and requests relief as set out below:

SUMMARY

1. AT&T brings this action to stop T-Mobile's willful, unlawful, and ongoing intrusion into AT&T's computer systems, which T-Mobile has persisted in even after AT&T told T-Mobile to stop. On November 20, 2025, T-Mobile announced the beta launch of a software tool called "Switch Made Easy" (SME), along with plans for a full launch of SME on December 1, 2025. SME uses an automated bot, operating under the guise of AT&T customers, to harvest private customer account information and AT&T business information from password-protected websites hosted on AT&T servers. Through the use of the SME bot, T-Mobile deliberately circumvents security measures on AT&T's non-public websites without AT&T's authorization.

[1] Defendant T-Mobile US, Inc. appears to be doing business as "T-Mobile USA, Inc." AT&T's complaint refers to defendant as T-Mobile US, Inc. based on its public SEC filings.

T-Mobile also violates several prohibitions in AT&T's publicly available Terms of Use, which govern the use of all of its public and private websites. T-Mobile's unauthorized and illegal access jeopardizes AT&T customers' data security and privacy and threatens irreparable harm to AT&T's business, reputation, and goodwill.

2. AT&T is a telecommunications company that currently provides wireless service to over 119 million customers. Critical to AT&T's success is the trust of its customers. AT&T prioritizes the security of customer data and takes comprehensive measures to ensure that its data is handled responsibly. These practices are multi-layered and proactive, especially when it comes to protecting customer data and internet-facing systems.

3. T-Mobile is a telecommunications company that also offers wireless service. But this case is not about competition for customers. Rather, it is about T-Mobile's unauthorized and deceitful intrusion into AT&T's computer systems with T-Mobile's T-Life App. The SME scraping tool—included in the T-Life App—induces AT&T customers to log into AT&T accounts. Once logged in, T-Mobile launches an automated data-scraping bot, disguised as an AT&T customer, to harvest private customer account information and AT&T business information from AT&T's computer systems. What's more, T-Mobile has misled AT&T's customers about the actual extent of the customer data T-Mobile obtains to develop offers. Based on AT&T's investigation to date, T-Mobile scrapes over 100 categories of personal account information from each AT&T customer and sends them to T-Mobile's servers. On information and belief, T-Mobile is retaining this AT&T customer data T-Mobile's own records, regardless of whether the customer becomes a T-Mobile customer. T-Mobile's wholesale scraping of AT&T data threatens customer security and privacy, including exposing AT&T customers to the risk of identity theft, fraud, or other illegal uses of their data.

4. On the day that AT&T learned of the SME scraping tool's intrusion into its computer systems, AT&T took new steps to protect its customer's data by developing and implementing additional security measures in an attempt to detect and block intrusions from T-Mobile's SME scraping tool into AT&T systems. AT&T sent a cease-and-desist letter demanding that T-Mobile stop its unauthorized access into AT&T's computer systems. But T-Mobile has willfully refused to cease and desist. Instead, T-Mobile has repeatedly ignored AT&T's requests and taken further deliberate actions to access its systems without authorization. When AT&T took additional technical security measures to protect its systems from T-Mobile's illegal attacks, T-Mobile acted swiftly within one day to hack around AT&T's extra security protections so it could continue its bad acts. After informing T-Mobile that its conduct is unauthorized, AT&T has twice implemented additional technical blocks to stop T-Mobile's intrusion into its systems, and after each instance T-Mobile has reengineered its SME scraping tool to bypass those security measures. T-Mobile continues to march towards full release of the SME scraping tool on December 1, 2025.

5. To protect its customers data and computer systems, AT&T has been left with no choice but seek the Court's intervention to halt T-Mobile's illicit behavior. AT&T's claims for relief are: (1) violation of the Computer Fraud and Abuse Act ("CFAA"), 18 U.S. Code § 1030; (2) violation of the Texas Computer Crimes, Texas Penal Code 33.02, Civil Code 143.001; (3) violation of the Comprehensive Computer Data Access and Fraud Act ("CDAFA"); (4) violation of the Georgia Computer Systems Protections Act – O.C.G.A. § 16-9-93; (5) breach of contract; (6) tortious interference with contractual relations; and (7) misappropriation. AT&T seeks to immediate and permanent injunctive relief, as well as damages for T-Mobile's unlawful conduct.

THE PARTIES

6. Plaintiff AT&T Mobility LLC is a Delaware limited liability company with its principal place of business in Atlanta, Georgia. AT&T Mobility LLC is an indirectly owned subsidiary of AT&T Inc. AT&T Mobility provides wireless services to AT&T's customers.

7. Plaintiff AT&T Services, Inc., is a Delaware corporation with its principal place of business in Dallas, Texas. AT&T Services, Inc. is a wholly owned subsidiary of AT&T Inc. AT&T Services owns many of the systems that are being intruded and scraped by T-Mobile's actions.

8. Defendant T-Mobile US Inc. is a Delaware corporation with its principal place of business in Bellevue, Washington. T-Mobile is registered to do business in the State of Texas and can be served with process through its registered agent, Corporation Service Company, 211 East 7th Street, Suite 620, Austin, Texas 78701.

JURISDICTION AND VENUE

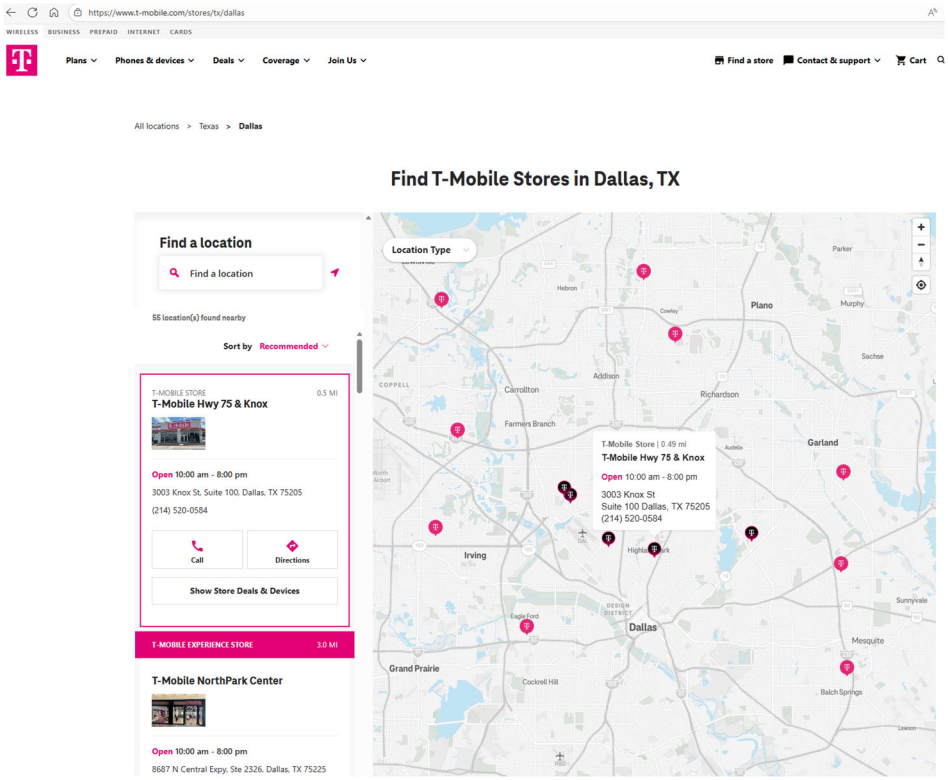
9. This Court has federal question subject-matter jurisdiction pursuant to 28 U.S.C. § 1331 over the CFAA cause of action alleged in this Complaint as the CFAA claim arises under 18 U.S. Code § 1030.

10. This Court has supplemental jurisdiction over the state law causes of action alleged in this Complaint pursuant to 28 U.S.C. § 1367, as the state law claims are so related to Plaintiffs' federal law claim that they form part of the same case or controversy and arise out of the same case or controversy as Plaintiffs' federal claim.

11. T-Mobile is subject to this Court's personal jurisdiction, consistent with the principles of due process and the Texas Long Arm Statute.

12. T-Mobile has sufficient minimum contacts and has engaged in continuous and systematic activities in the forum as a result of business conducted within this District and State of Texas. By way of example and without limitation, T-Mobile operates multiple brick-and-mortar

retail stores in the Northern District of Texas and over 400 stores in the State of Texas. These retail stores are physically located within this District, are regular and established places of business of T-Mobile, and are used by T-Mobile to actively market, sell, and provide products and services to local residents. T-Mobile's website provides a "Find your nearest T-Mobile store in Texas" feature that shows the location of T-Mobile retail stores within this District.



See, e.g., https://www.t-mobile.com/stores/tx/dallas (last visited November 26, 2025); *see also*, https://www.t-mobile.com/stores/tx (last visited November 26, 2025).

13. T-Mobile also maintains multiple "T-Mobile Corporate Offices" in Texas, including one located at 3560 Dallas Pkwy, Frisco, TX 75034. Through the physical storefronts and corporate office, T-Mobile purposefully avails itself of the privileges of conducting business in Texas.

14. T-Mobile maintains a substantial and continuous presence in Texas and this District, which extends well beyond its physical retail locations. In addition to operating brick-

and-mortar stores, T-Mobile owns and operates nationwide telecommunications networks that reach customers throughout Texas, including within this District. T-Mobile owns, operates, and maintains a substantial telecommunications network infrastructure within this forum, including cellular towers, fiber-optic cabling, and switching stations. Through these networks and infrastructures, T-Mobile provides a broad range of telecommunication services—voice, data, mobile, and related digital features and tools—directly to residents and businesses in this District and Texas.

15. The SME scraping tool and T-Life App at issue are part of the same suite of offerings that T-Mobile actively markets, delivers, and supports in this District and Texas. T-Mobile has purposefully availed itself of the laws and jurisdiction of Texas because, among other things, it provided or made available, or will provide or make available, the SME scraping tool and T-Life App (including beta and full versions) to residents (including all current AT&T customers) of this District and Texas, as well as support services, including troubleshooting, activation, and technical support regarding the SME scraping tool and T-Life App. Its website prominently advertises the SME scraping tool and T-Life App—through which users can access and manage their accounts, including AT&T consumers. These tools, applications, and websites are not passive; they are purposefully directed at residents of this District and Texas, and are structured to facilitate commercial transactions here, including encouraging the residents to log in, utilize the SME scraping tool and T-Life App, and switch to T-Mobile's plans. T-Mobile's in-state retail presence further underscores its intent to cultivate and serve a customer based in this District and Texas. By soliciting potential customers and providing on-site service within this District for the SME scraping tool and T-Life App that are at issue in this case, T-Mobile has established sufficient minimum contacts to subject it to personal jurisdiction in this Court.

16. Moreover, the claims in this case arise directly out of, or at a minimum relate closely to, T-Mobile's forum-directed activities. T-Mobile has targeted AT&T's systems, which are located in large part in the Northern District in Texas. T-Mobile also is intentionally targeting residents of this District and Texas—including AT&T's customers—and inducing them to access their accounts and interact with the very feature that is the subject of the dispute. T-Mobile also supports and services these customers through its brick-and-mortar operations within this District and Texas. Sufficient nexus exists between T-Mobile's contacts with the forum and the claims alleged in this complaint.

17. T-Mobile's business activities in this District and Texas are neither isolated nor incidental—it does significant business here. It maintains a Texas registered agent, pays Texas franchise taxes, and maintain an extensive physical presence, including large-scale infrastructure facilities, hundreds of retail stores, and a corporate office in Frisco. T-Mobile also maintains extensive customer relationships locally, collects revenue from subscribers in this District, and continuously transmits signals, data, and communications over infrastructure that it controls and manages in this District and Texas. It also engages in targeted advertising, customer service operations, and ongoing contractual relationships with residents of this District and Texas, including employing hundreds if not thousands of Texans. By purposefully directing its commercial activities toward this forum and deriving substantial benefits from doing so, T-Mobile has established the requisite minimum contacts for the exercise of personal jurisdiction. Further, by soliciting subscribers in this forum and utilizing its local network to deliver service to residents here, as well as attacking AT&T's computer systems with automated tools to gain unauthorized

access to AT&T's systems here, T-Mobile created a substantial connection with this District, making the exercise of personal jurisdiction both foreseeable and reasonable.[2]

18. Plaintiffs maintain a place of business within this District. For example, AT&T Services, Inc. has its headquarters within this District at 208 S. Akard Street, Dallas, TX 75202.

19. Venue is proper in this District pursuant to 28 U.S.C. § 1391 because of the same reasons that personal jurisdiction is proper as discussed above and because the claims asserted in this action arose in this District and a substantial part of the activities, conduct and damages have occurred in this District. In addition,

FACTUAL BACKGROUND

I. AT&T's Comprehensive Measures to Protect Customer Data and Privacy

20. AT&T is an American telecommunications company that provides wireless service to over 119 million customers. Critical to AT&T's success is the trust of its customers. As part of AT&T's ongoing efforts to build and maintain that trust, AT&T invests continually in the best technology and practices to protect customer data, comply with all applicable privacy regulations, and prevent unauthorized access, misuse, and other threats to AT&T's systems.

21. AT&T believes that customers should be empowered with transparent information about pricing and services. To that end, AT&T provides customers with ready but protected access to detailed data about their user accounts, contracts, wireless plans, billing and billing history, promotions, and subscriptions. One way customers can access their AT&T account data is through

---

[2] *See* https://www.t-mobile.com/coverage/coverage-map (showing that T-Mobile provides 5G service in Texas) (last visited November 26, 2025); *see also* https://www.t-mobile.com/news/network/t-mobile-bringing-more-to-texas; https://www.t-mobile.com/news/press/new-stores-in-dallas-fort-worth; https://careers.t-mobile.com/?location_name=Dallas&location_type=1 (showing T-Mobile's job openings near Dallas) (last visited November 26, 2025); https://careers. t-mobile.com/jobs?filter%5Bstate%5D%5B0%5D=Texas (showing T-Mobile's job openings in Texas) (last visited November 26, 2025).

password-protected accounts on the non-public portions of AT&T's websites. For example, customers can access their AT&T account after providing their username and password at https://signin.att.com/.

22. Consistent with AT&T's belief in the importance of transparency and choice, AT&T customers can share information about their service plans and compare their AT&T plans with those of their competitors. By way of example, customers can download their bills and, using those bills, compare pricing and services, including on AT&T's competitor websites.

23. AT&T also prioritizes the security of customer data and takes comprehensive measures to ensure that its data is handled responsibly. These practices are multi-layered and proactive, especially when it comes to protecting customer data and internet-facing systems. Both AT&T's Terms of Use ("TOU") governing its websites, both the public and non-public portions, and additional computer security measures seek to prevent unauthorized access to AT&T's systems. The TOU applies to the AT&T plaintiff entities in this complaint as both are "subsidiaries and affiliates of AT&T Inc."

24. AT&T also implements a range of advanced, continuous security measures to (1) detect and block unauthorized access to AT&T's systems, (2) absorb and mitigate actions that threaten the operation and integrity of publicly accessible applications, and (3) shield against common web exploits and efforts to harvest and abuse private information stored within AT&T's systems.

25. AT&T's TOU is publicly available on each page of AT&T's website. It applies to everyone accessing AT&T's websites and includes many provisions designed to safeguard customer private information, as well as to maintain the integrity of AT&T's computer systems. Every visitor, including T-Mobile, agrees to the TOU when it accesses and uses the website.

AT&T's TOU at § 1 ("by accessing or using our site in any way you are agreeing to comply with these Terms of Use").[3] For example, AT&T's TOU prohibit any activity that:

- "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;
- "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";
- " . . . exploits for any commercial purposes, any portion of the Sites or Content";
- "collects and uses any Content, including the use of any data mining, or similar data gathering or extraction methods." *Id.* at § 14.

Id. at § 14. The TOU further states that "[e]xamples of security violations include, without limitation, unauthorized access to or use of data or systems including . . . unauthorized monitoring of data or traffic." *Id.* at § 15.

26. T-Mobile is well aware of the TOU's requirements. It is a sophisticated competitor that, on information and belief, closely monitors AT&T. And there can be no doubt of its awareness because on November 24, 2025, AT&T directed T-Mobile to the specific language in the TOU discussed above.

27. Nor can T-Mobile be surprised by or reasonably dispute the applicability and importance of those provisions, T-Mobile prohibits the same conduct it is employing against AT&T. T-Mobile's own website has similar prohibitions against activities that "bypass or circumvent measures we may use to prevent, interfere, or limit access to the Site or any T-Mobile network," "use the Site to intercept, collect or store personal information about other users," or

[3] https://www.att.com/legal/terms.attWebsiteTermsOfUse.html?

"access, monitor or copy any content or information on the Site using any robot, spider, scraper or other automated means or any manual process."[4]

II. T-Mobile's SME Scraping Tool Scrapes AT&T's Data

28. T-Mobile made available its "T-Life App" in early 2024, which has been installed over 90 million times and can be installed on any wireless device regardless of whether the device currently uses T-Mobile or another carrier, such as AT&T, for telecommunications services.

29. On November 20, 2025, T-Mobile announced the introduction of the SME scraping tool, as a new tool in the T-Life App.[5]

30. With the SME scraping tool, T-Mobile asks users to provide T-Mobile with their AT&T login and password in the SME scraping tool:

> "With Easy Switch (beta)[6], **any wireless customer can open T-Life**, **log in to their current AT&T** and Verizon wireless provider — and based on their number of lines, devices and plan — it will identify and recommend the best plans for that customer"[7]

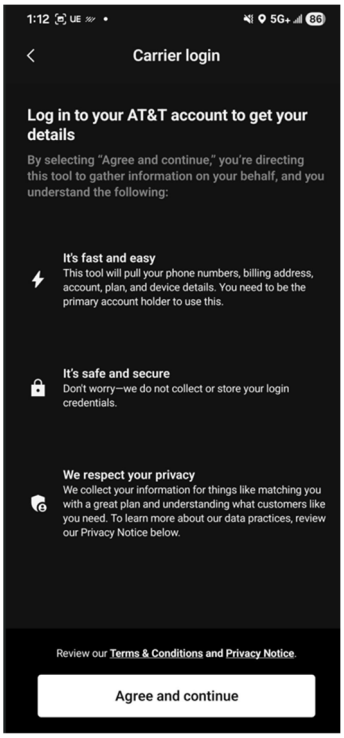
T-Mobile accesses the customer's AT&T account and launches an automated data-scraping bot against AT&T's computer systems to conduct wholesale scraping of much more than "number of lines, devices, and plan." In truth, T-Mobile scrapes over 100 fields of that customer's personal account information, contracts, phones and phone plans, billing and billing history, among others sensitive and private information. Significantly, this includes information relating to other individuals on the customer's account (such as family members) and AT&T products or services beyond just wireless services. T-Mobile's illegal bot does not accurately identify itself to AT&T;

---

[4] https://www.t-mobile.com/responsibility/consumer-info/policies/terms-of-use?
[5] https://www.t-mobile.com/news/un-carrier/switchingmadeeasy?
[6] Notably, T-Mobile refers to its SME scraping tool interchangeably as Easy Switch and Switch Made Easy.
[7] https://www.t-mobile.com/news/un-carrier/switchingmadeeasy?

rather it disguises itself to appear to be a generic web browser, hoping to trick AT&T's computer systems into thinking that the connection is from a legitimate customer—rather than by T-Mobile engaging in prohibited and illegal intrusion into its systems and data extraction.

31. T-Mobile purports to use that data to develop an offer for a competing service from T-Mobile. T-Mobile also states that it would use the information gathered from AT&T's computer systems to gather information about "what [AT&T] customers like you need":



32. T-Mobile is not authorized by AT&T to access its systems and scrape this data, and AT&T has informed T-Mobile of that expressly.

33. T-Mobile's SME scraping tool is currently in beta mode.[8] T-Mobile has announced plans to make the tool widely available on December 1, 2025. *Id.*

[8] *Id.*

III. T-Mobile's Circumvention of AT&T's Security Measures and Defiance of AT&T Cease-and-Desist Letter

34. Immediately after the beta release of T-Mobile's SME scraping tool on November 20, 2025, AT&T began detecting unauthorized intrusions into AT&T's systems and scraping of AT&T customer account data. AT&T's investigation shows that T-Mobile's SME scraping tool accesses and copies confidential data from password-protected AT&T websites hosted on AT&T's servers in Dallas, Texas, Alpharetta, Georgia, and Fairfield, California. The SME scraping tool then sends back to T-Mobile over 100 data fields about AT&T's customers, including full legal name, billing and physical addresses, billing and billing history, phones and devices, trade-in values, installment plans and payoffs, available upgrades and upgrade pathways, charges and disputes, among many other fields.

35. AT&T's investigation further shows that T-Mobile intentionally designed its SME scraping tool to hide its unauthorized access to AT&T's systems. When the SME scraping tool sends AT&T customer data scraped from AT&T's servers back to the T-Mobile's servers, the response data includes fields identifying the data as associated with T-Mobile's T-Life App name, *i.e.*, "Origin-Application-Id=TLIFE." But when the SME scraping tool accesses AT&T's systems and issues requests to scrape AT&T's customer data, the SME scraping tool and T-Mobile's automated bot intentionally omits any identification information associating itself with T-Life or T-Mobile, in a blatant attempt to avoid detection as an unauthorized intrusion.

36. Upon discovery of T-Mobile's intrusions, AT&T immediately began to develop and implement new security measures to detect and block T-Mobile's unauthorized access to AT&T's systems, including by detecting patterns or behaviors associated with the SME scraping tool. AT&T designed these measures to prevent unauthorized access, while still permitting legitimate customers to view their account information.

37. On November 24, 2025, four days after the launch of the SME scraping tool on November 20, 2025, AT&T sent a cease-and-desist letter demanding that T-Mobile stop its unauthorized access to AT&T's systems. AT&T's letter makes clear that T-Mobile's use of the SME scraping tool to access AT&T's systems is unauthorized, not permitted by AT&T, and also a breach of AT&T's TOU. AT&T further explained that T-Mobile's use of the SME scraping tool to gain unauthorized access to AT&T's systems also violates federal and state laws.

38. AT&T's actions to protect against unauthorized access is fully consistent with its vigilant data-security practices to protect customer data and its business information. It regularly protects its systems from bots or other bad actors and does not allow scraping of non-public information.

39. Right after SME's launch, AT&T began detecting intrusions by SME's scraping tool and developing blocking measures, which were implemented and rolled out on November 24. On the afternoon of November 25, less than a day after AT&T implemented its additional security blocking measures to prevent T-Mobile's illegal scraping, AT&T detected that T-Mobile had modified T-Life and disguised the identity of its requests to circumvent AT&T's new security blocking measures. T-Mobile intentionally reengineered T-Life to evade AT&T's security measures even after it was put on notice by AT&T through the November 24 cease-and-desist letter that such conduct was unauthorized. After discovering T-Mobile's misconduct, on the evening of November 25, AT&T developed and implemented yet additional security blocking measures to prevent T-Mobile's unauthorized access to its systems. Despite twice blocking through security measures T-Mobile's data-scraping app, on November 26, T-Mobile once again modified and disguised T-Life to attempt to circumvent the security measures that AT&T had implemented to prevent unauthorized access to its systems. AT&T has since been forced once

again to develop and implement security measures to prevent T-Mobile's unauthorized intrusion and data scraping. On information and belief, and based on T-Mobile's course of conduct to date, AT&T anticipates that T-Mobile will continue to develop techniques to circumvent AT&T's security measures, at substantial harm to AT&T and its customers, absent judicial intervention.

COUNT I

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

40. AT&T realleges and incorporates the allegations of paragraphs 1 – 39 of this Complaint.

41. AT&T's servers and computer systems are computers that are used in or affecting interstate or foreign commerce or communication, and they are thus protected computers under 18 U.S.C. § 1030(e)(2)(B).

42. T-Mobile has violated 18 U.S.C. § 1030(a)(2) because it knowingly and intentionally accessed, and continues to access, AT&T's servers without authorization or in excess of authorization, obtaining password-protected customer account information from non-public AT&T websites hosted on AT&T's protected computers. The customer account data that T-Mobile has obtained is vast, spanning over 100 different data fields, and including such information as full legal name, billing and physical address, billing and billing history, phones and devices, trade-in values, installment plans and payoffs, available upgrades and upgrade pathways, and charges and disputes, to name just a few categories of data.

43. T-Mobile's access to AT&T's servers has been without authorization or in excess of authorization, because it is in violation of AT&T's TOU, which prohibits automated scraping, commercial exploitation of data accessed through AT&T's websites, and circumvention of AT&T's security measures. T-Mobile has had constructive knowledge of AT&T's TOU (as a sophisticated commercial entity that maintains its own terms of use containing similar

prohibitions), which has been in place since January 2020, and is publicly available online at https://www.att.com/legal/terms.attWebsiteTermsOfUse.html. In addition, T-Mobile received actual notice and knowledge by no later than November 24, 2025, through the cease-and-desist letter sent by AT&T on that date, demanding that T-Mobile stop its unauthorized access to AT&T's systems. T-Mobile's continued access to and use of AT&T's websites after T-Mobile's constructive and actual knowledge of the TOU confirm T-Mobile's agreement to the TOU.

44. T-Mobile's own conduct further demonstrates T-Mobile's knowledge that its conduct described above is unauthorized or exceeds authorized access. T-Mobile's T-Life App attempts to conceal its identity from AT&T's servers, while performing its unauthorized and illegal scraping, and T-Mobile has deliberately circumvented multiple technical security measures that AT&T has employed, including both measures in place since before T-Mobile's beta-testing of the SME scraping tool began, as well as the additional security measures in place since November 24, 2025, to prevent its automated scraping.

45. T-Mobile also has violated 18 U.S.C. § 1030(a)(4) because it knowingly, and with intent to defraud, accessed, and continues to access, AT&T's servers without authorization or in excess of authorization, and by means of such conduct has furthered the intended fraud and obtained something of value. T-Mobile's intended fraud has included sending commands and requests to AT&T's servers that omit information that could identify those commands and requests as originating from the SME scraping tool, T-Mobile, or an automated bot, and instead falsely indicate that they originate from authenticated logged-in customers, in order to access and obtain password-protected customer account data from AT&T.

46. T-Mobile's conduct has caused a loss to AT&T as defined by 18 U.S.C. § 1030(e)(11), during a one-year period in excess of $5,000, including AT&T's substantial expenditure of resources to investigate and remediate T-Mobile's conduct.

47. AT&T has suffered immediate irreparable and incalculable harm resulting from T-Mobile's conduct, and—as demonstrated by its disregard of AT&T's November 24, 2025 letter and security measures—T-Mobile's misconduct and resulting harm will continue unless T-Mobile is enjoined from further unauthorized access and use of AT&T's protected computers.

48. AT&T also seeks compensatory damages in an amount to be proven at trial and injunctive relief under 18 U.S.C. § 1030(g).

COUNT II

Texas Computer Crimes – Tex. Civ. Practice and Remedies Code 143.001

49. AT&T realleges and incorporates the allegations of paragraphs 1 – 48 of this Complaint.

50. T-Mobile knowingly and intentionally accessed, and is continuing to access, AT&T's servers—including those located in Texas—without AT&T's effective consent, in violation of Texas Penal Code § 33.02. T-Mobile's access to AT&T's systems has been without effective consent because: it is in violation of AT&T's TOU, which prohibits automated scraping, commercial exploitation of data accessed through AT&T's websites; it disregards AT&T's November 24, 2025 cease and desist letter that expressly rejected any authorization for T-Mobile misconduct based on the SME scraping tool; and it repeatedly circumvents AT&T's security measures, including those in place since before T-Mobile began beta-testing the SME scraping tool and those that were implemented on November 24, 2025, and then again on November 25, 2025.

51. As a sophisticated commercial entity that maintains its owns terms of use containing similar prohibitions to those at issue here, T-Mobile has had constructive knowledge that its access to AT&T's servers lacked effective consent. Moreover, T-Mobile has had actual knowledge that it lacked effective consent, at least by November 24, 2025, when it received AT&T's cease-and-desist letter rejecting any authorization by AT&T and demanding that it cease its unauthorized access and scraping of AT&T's password-protected webpages.

52. Through the SME scraping tool and automated bots, T-Mobile obtained access to AT&T's private customer data and confidential business information, as a result of which, AT&T has lost control over its computer servers and customer data. Thus, T-Mobile accessed AT&T's servers with the intent and effect of causing harm to AT&T.

53. AT&T has been and will continue to be damaged as the result of T-Mobile's violation of the Texas Penal Code.

54. Pursuant to § 143.001 of the Texas Civil Practice and Remedies Code, T-Mobile's knowing and intentional violation of Texas Penal Code § 33.02 makes T-Mobile liable for the harmful access of AT&T's servers.

55. As a direct and proximate result of T-Mobile's conduct, AT&T is entitled to damages in an amount to be proven at trial pursuant to Texas Civil Practice and Remedies Code § 143.002 and otherwise according to law. AT&T is further entitled to its attorneys' fees and full costs pursuant to Texas Civil Practice and Remedies Code § 143.002 and otherwise according to law.

56. AT&T has suffered irreparable and incalculable harm resulting from T-Mobile's conduct, and this harm will continue unless T-Mobile is enjoined from further unauthorized access and use of AT&T's protected computers.

COUNT III

Violation of the Comprehensive Computer Data Access and Fraud Act ("CDAFA") – Cal. Penal Code § 502 *et seq.*

57. AT&T hereby realleges and incorporates the allegations of paragraphs 1 – 56 of this Complaint.

58. AT&T also owns servers located in California that have been targeted by T-Mobile's scraping activities, and AT&T is able to bring a cause of action under Cal. Penal Code § 502. This cause of action is in addition to and in the alternative to a Texas cause of action, with respect to the affected California-based servers.

59. Cal. Penal Code § 502 provides: "For purposes of bringing a civil or a criminal action under this section, a person who causes, by any means, the access of a computer, computer system, or computer network in one jurisdiction from another jurisdiction is deemed to have personally accessed the computer, computer system, or computer network in each jurisdiction."

60. T-Mobile violated Cal. Penal Code § 502(c)(2) by knowingly and without permission accessing password protected websites hosted on AT&T's servers and scraping AT&T's customer data and business information from those secure websites and servers. T-Mobile accessed, copied, took, analyzed, and used data from AT&T's servers in and from the State of California. On information and belief, at least some of AT&T's servers used to host secure websites and the private customer data that has been scraped by T-Mobile's SME scraping tool and bots are located in California.

61. T-Mobile also violated Cal. Penal Code § 502(c)(3) by knowingly and without permission using AT&T's computer services, as defined by § 502(b)(4). T-Mobile used AT&T's servers to access and copy the data it scraped from those servers.

62. As a sophisticated commercial entity that maintains its owns terms of use containing similar prohibitions to aAT&T's terms, T-Mobile has had constructive knowledge that it lacked authorization to access AT&T's servers in the manner alleged. Moreover, T-Mobile has had actual knowledge that its access is unauthorized, at least by November 24, 2025, when it received AT&T's cease-and-desist letter rejecting any authorization by AT&T and demanding that it cease its unauthorized access and scraping of AT&T's password-protected webpages.

63. As a direct and proximate result of T-Mobile's conduct, AT&T has suffered damages, including but not limited to AT&T's substantial expenditure of resources to investigate and remediate T-Mobile's conduct.

64. AT&T has suffered immediate irreparable and incalculable harm resulting from T-Mobile's conduct, and—as demonstrated by its disregard of AT&T's November 24, 2025 letter and security measures—T-Mobile's misconduct and resulting harm will continue unless T-Mobile is enjoined from further unauthorized access and use of AT&T's protected computers.

65. AT&T is entitled to compensatory damages, and/or disgorgement in an amount to be proven at trial, and declarative, injunctive, or other equitable relief.

66. AT&T is also entitled to recover its reasonable attorneys' fees pursuant to Cal. Penal Code § 502(e).

COUNT IV

Violation of the Georgia Computer Systems Protections Act – O.C.G.A. § 16-9-93

67. AT&T realleges and incorporates the allegations of paragraphs 1 – 66 of this Complaint.

68. AT&T maintains corporate offices and retail locations within Georgia, and AT&T owns and operates additional servers located in Alpharetta, Georgia, that, on information and belief, have been targeted by T-Mobile's scraping activities.

69. O.C.G.A. § 16-9-93(g) provides: "Any person whose property or person is injured by reason of a violation of any provision of this article may sue therefor and recover for any damages sustained and the costs of suit."

70. T-Mobile violated O.C.G.A. § 16-9-93(a), by using AT&T's computer systems with knowledge that such use was without authority, to scrape AT&T's password-protected customer data. On information and belief, T-Mobile accessed, copied, took, analyzed, and used data from AT&T's servers in and from the State of Georgia.

71. As a sophisticated commercial entity that maintains its owns terms of use containing similar prohibitions to AT&T's terms, T-Mobile has had constructive knowledge that it lacked authorization to access AT&T's computer systems in the manner alleged. Moreover, T-Mobile has had actual knowledge that it's access is unauthorized, at least by November 24, 2025, when it received AT&T's cease-and-desist letter rejecting any authorization by AT&T and demanding that it cease its unauthorized access and scraping of AT&T's password-protected webpages.

72. As a direct and proximate result of T-Mobile's conduct, AT&T has suffered damages, including but not limited to AT&T's substantial expenditure of resources to investigate and remediate T-Mobile's conduct.

73. AT&T is entitled to compensatory and punitive damages, and such other and further relief as the Court deems just and proper

COUNT V

Breach of Contract

74. AT&T realleges and incorporates the allegations of paragraphs 1 – 73 of this Complaint.

75. Access and use of AT&T's websites, including both public and non-public websites, is governed by and subject to AT&T's Terms of Use (TOU).

76. AT&T's TOU applies to websites operated by the subsidiaries and affiliates of AT&T Inc., including both AT&T Mobility LLC and AT&T Services, Inc.

77. AT&T's TOU constitutes a valid and enforceable contract between AT&T and anyone who accesses or uses AT&T's websites. This includes T-Mobile, who has used its T-Life app to access password-protected portions of AT&T websites hosted on AT&T's servers.

78. At all relevant times, T-Mobile has had constructive or actual knowledge of AT&T's TOU.

79. T-Mobile is a sophisticated commercial entity that operates its own websites subject to its own terms of use, which includes restrictions against data scraping and circumvention of security measures similar to those at issue here. As such, T-Mobile knew or should have known that AT&T's websites would likewise be governed by terms of use prohibiting similar misconduct. AT&T's TOU was, at all relevant times, readily and publicly available to T-Mobile by means of a clear hyperlink posted on AT&T's websites.

80. T-Mobile has also had actual notice and knowledge of AT&T's TOU by no later than November 24, 2025, when it received AT&T's cease-and-desist letter expressly informing T-Mobile that its unauthorized access and scraping of AT&T's password-protected webpages is in violation of AT&T's TOU, and demanding that it cease this conduct.

81. Through its continued access of AT&T's websites, with actual and constructive knowledge of the TOU, T-Mobile has agreed to AT&T's TOU. The TOU includes provisions prohibiting, among other things, any activity that: (1) uses any robot, spider, or other such programmatic or automatic device to obtain information from AT&T's websites or otherwise

monitor or copy any portion of those websites, products or services; (2) uses, downloads or otherwise copies any user information and/or usage information or any portion thereof, or transmits, provides or otherwise distributes such information to any third party; (3) exploits for any commercial purposes, any portion of AT&T's websites, or of content available through those websites; or (4) collects and uses any content available through AT&T's websites, including the use of any data mining, or similar data gathering or extraction methods.

82. AT&T has performed all obligations required of it under the TOU.

83. T-Mobile has breached AT&T's TOU by using its SME scraping tool and unidentified automated bots to harvest private customer account information and AT&T business information for AT&T's password-protected websites.

84. Despite having actual and constructive knowledge that its conduct violates AT&T's TOU, T-Mobile has continued to willfully, repeatedly, and materially breach the TOU.

85. As a direct and proximate result of T-Mobile's breaches, AT&T has suffered damages, including but not limited to AT&T's substantial expenditure of resources to investigate and remediate T-Mobile's conduct.

86. AT&T has suffered immediate irreparable and incalculable harm resulting from T-Mobile's conduct, and—as demonstrated by its disregard of AT&T's November 24, 2025 letter and its security measures—T-Mobile's misconduct and resulting harm will continue unless T-Mobile is enjoined from further unauthorized access and use of AT&T's protected computers.

87. AT&T is entitled to compensatory damages, restitution as permitted, injunctive relief enforcing specific performance of the TOU, costs, and such other and further relief as the Court deems just and proper.

COUNT VI

TORTIOUS INTERFERENCE WITH CONTRACT

88. AT&T realleges and incorporates the allegations of paragraphs 1 – 87 of this Complaint.

89. AT&T's TOU is a valid and enforceable contract between AT&T and its customers, which governs access and use of AT&T's websites, including the password-protected websites through which AT&T customers can view their account data. AT&T customers who register for an account on AT&T's password-protected customer portal are informed of, and must affirmatively agree to, AT&T's TOU, as part of the registration process.

90. At all relevant times, T-Mobile has known of the existence and applicability of AT&T's TOU to the access and use of AT&T's password-protected webpages by AT&T's customers. T-Mobile is a sophisticated commercial entity that operates its own websites subject to its own terms of use, which includes restrictions against data scraping and circumvention of security measures similar to those at issue here. As such, T-Mobile knew or should have known that AT&T's websites would likewise be governed by terms of use prohibiting similar misconduct. AT&T's TOU was, at all relevant times, readily and publicly available to T-Mobile by means of a clear hyperlink posted on AT&T's websites.

91. Moreover, T-Mobile itself had actual notice and knowledge of AT&T's TOU by no later than November 24, 2025, when it received AT&T's cease-and-desist letter expressly informing T-Mobile that its unauthorized access and scraping of AT&T's password-protected webpages is in violation of AT&T's TOU, and demanding that it cease this unauthorized conduct.

92. With knowledge of AT&T's contractual relationships with its customers, T-Mobile has intentionally encouraged and induced AT&T customers to breach AT&T's TOU by duping them. By offering the SME scraping tool without disclosing to AT&T customers that T-Mobile will be unlawfully using disguised bots that are prohibited by the TOU to scrape AT&T's computer

systems, T-Mobile has deceptively implied to customers that use of the SME scraping tool is consistent with the TOU. In addition, by telling AT&T's customers that T-Mobile will not "collect or store" their login credentials and that T-Mobile is merely collecting information to match them with a plan, T-Mobile has misled AT&T's customers about the actual extent of T-Mobile's data harvesting, through which T-Mobile is scraping over a hundred categories of personal account information that, on information and belief, T-Mobile is retaining in its own company's records, regardless of whether the customer becomes a T-Mobile customer. In this manner, T-Mobile has induced and caused AT&T customers to log into AT&T's password-protected webpages to use T-Mobile's SME scraping tool, which enable T-Mobile's automated bots to scrape data from AT&T's password-protected webpages, in violation of AT&T's TOU.

93. As a direct and proximate result of T-Mobile's interference with AT&T's contractual relations that protect AT&T's systems and data from scraping by bots, AT&T has suffered damages, including but not limited to AT&T's substantial expenditure of resources to investigate and remediate T-Mobile's conduct.

94. AT&T has suffered immediate irreparable and incalculable harm resulting from T-Mobile's conduct, and—as demonstrated by its disregard of AT&T's November 24, 2025 letter and its security measures—T-Mobile's misconduct and resulting harm will continue unless T-Mobile is enjoined from further unauthorized access and use of AT&T's protected computers.

95. AT&T is entitled to compensatory and punitive damages, restitution as permitted, injunctive relief enforcing specific performance of the TOU, costs, and such other and further relief as the Court deems just and proper.

COUNT VII: MISAPPROPRIATION

96. AT&T hereby realleges and incorporates the allegations of paragraphs 1 – 95 of this Complaint.

97. AT&T places a high value on the trust of its customers, continually investing in the best technology and practices to protect customer data, comply with all applicable privacy regulations, and prevent unauthorized access, misuse, and other threats to its systems.

98. At the same time, AT&T believes that customers should be empowered with transparent information about pricing and services. To that end, AT&T has developed systems and websites to provide its customers with detailed data about their user accounts, contracts, wireless plans, billing and billing history, promotions, and subscriptions. Customers are able to access their AT&T account data through password-protected accounts on the non-public portions of AT&T's websites.

99. AT&T has invested substantial time, effort, and money in developing both its customer relationships, as well as the websites and computer systems it has put in place to support its customers. In particular, AT&T has developed hosting infrastructure, security systems, and specialized software, to gather, curate, and make available personal account data to its customers, in real time, through its password-protected webpages. This account data is time-sensitive, non-public, commercially valuable data gathered and stored by AT&T at considerable expense. Without authorization, T-Mobile has accessed AT&T's password-protected systems to scrape AT&T's time-sensitive customer data. T-Mobile has publicly stated that it is doing this to gather competitive intelligence about AT&T's customer base. Thus, T-Mobile seeks to gain a competitive advantage over AT&T, by free-riding on AT&T's efforts, misappropriating both AT&T's password-protected customer data and the systems AT&T has developed to provide that data to its customers..

100. As a direct and proximate result of T-Mobile's misappropriation of AT&T's systems and data, AT&T has suffered harms, including but not limited to AT&T's substantial

expenditure of resources to investigate and remediate T-Mobile's conduct, and damage to AT&T's reputation and goodwill with its customers.

101. AT&T is entitled to compensatory and punitive damages, restitution as permitted, injunctive relief enforcing specific performance of the TOU, costs, and such other and further relief as the Court deems just and proper.

REQUEST FOR RELIEF

AT&T respectfully requests judgment in its favor and against T-Mobile as follows:

AT&T requests that the Court issue temporary, preliminary, and permanent injunctive relief, enjoining and restraining T-Mobile and its agents, employees, successors, and assigns, and all other persons acting in concert with or in conspiracy with or affiliated with T-Mobile, from:

a. Accessing, attempting to access, or assisting, instructing, or providing a means for others to access or attempt to access AT&T's protected computer systems and password protected websites using automated means without authorization.

b. Using any customer accounts on AT&T's websites, or inducing AT&T customers to allow use of their accounts, for the purpose of allowing T-Mobile's applications or automated tools to access AT&T's protected computer systems and password protected websites;

c. Accessing, attempting to access, or assisting, instructing, or providing a means for others to access AT&T's protected computer systems and password protected websites, in excess of AT&T's authorization;

d. Violating or evading any technological measures, barriers, or restrictions AT&T puts on the use of automated tools for accessing or obtaining customer data from AT&T's protected computer systems and password protected websites; and

e. Violating the terms of AT&T's TOU for its websites or any other application AT&T terms of use or service terms (including any future updates or amendments to those terms), and preventing further interference by AT&T with AT&T's contractual relationships, including with AT&T customers.

AT&T further requests that the Court order the following additional nonmonetary relief:

a. Inventory, accounting, and destruction of by T-Mobile of all copies of AT&T's data, including customer data, unlawfully obtained by T-Mobile, whether in the custody or control of T-Mobile or its employees, agents, assigns, or the third-party service providers (including, without limitation, web hosts, cloud providers, proxy servers, privacy services, and domain registrars);

b. Identification of each AT&T customer account ever accessed, used, or controlled through or by T-Mobile, or any of its employees, agents, and assigns, to engage in the complained-of conduct; and

c. That T-Mobile certify and confirm, in writing and under oath, within thirty days of the issuance of any order of the Court providing a remedy to AT&T, that T-Mobile has complied fully and completely with all requirements of such order.

AT&T further requests that the court award to AT&T as permitted by law and in such amounts to be proven at trial:

a. Monetary damages, including but not limited to compensatory, statutory, and punitive damages;

b. AT&T's reasonable costs, including reasonable attorneys' fees; and

c. Pre- and post-judgment interest.

AT&T further requests such other relief as the Court may deem just and proper.

JURY DEMAND

Pursuant to Federal Rule of Civil Procedure 38, Plaintiffs demand a jury trial on all issues and claims so triable.

Dated: November 26, 2025

O'MELVENY & MYERS LLP

By: /s/ *Timothy S. Durst*

TIMOTHY S. DURST
tdurst@omm.com
SID MODY
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

JS 44 (Rev. 04/21) (TXND 4/21)

CIVIL COVER SHEET

The JS 44 civil cover sheet and the information contained herein neither replace nor supplement the filing and service of pleadings or other papers as required by law, except as provided by local rules of court. This form, approved by the Judicial Conference of the United States in September 1974, is required for the use of the Clerk of Court for the purpose of initiating the civil docket sheet. *(SEE INSTRUCTIONS ON NEXT PAGE OF THIS FORM.)*

I. (a) PLAINTIFFS

AT&T Services Inc.

AT&T Mobility LLC

(b) County of Residence of First Listed Plaintiff Dallas County, Texas
(EXCEPT IN U.S. PLAINTIFF CASES)

(c) Attorneys *(Firm Name, Address, and Telephone Number)*

Timothy S. Durst, O'Melveny & Myers LLP, 2801 North Harwood Street, Suite 1600, Dallas, Texas, 75201,

DEFENDANTS

T-Mobile US Inc.

County of Residence of First Listed Defendant King County, WA
(IN U.S. PLAINTIFF CASES ONLY)

NOTE: IN LAND CONDEMNATION CASES, USE THE LOCATION OF THE TRACT OF LAND INVOLVED.

Attorneys *(If Known)*

II. BASIS OF JURISDICTION *(Place an "X" in One Box Only)*

- ☐ 1 U.S. Government Plaintiff
- ☒ 3 Federal Question *(U.S. Government Not a Party)*
- ☐ 2 U.S. Government Defendant
- ☐ 4 Diversity *(Indicate Citizenship of Parties in Item III)*

III. CITIZENSHIP OF PRINCIPAL PARTIES *(Place an "X" in One Box for Plaintiff and One Box for Defendant)*

(For Diversity Cases Only)

	PTF	DEF		PTF	DEF
Citizen of This State	☐ 1	☐ 1	Incorporated *or* Principal Place of Business In This State	☐ 4	☐ 4
Citizen of Another State	☐ 2	☐ 2	Incorporated *and* Principal Place of Business In Another State	☐ 5	☐ 5
Citizen or Subject of a Foreign Country	☐ 3	☐ 3	Foreign Nation	☐ 6	☐ 6

IV. NATURE OF SUIT *(Place an "X" in One Box Only)*

Click here for: Nature of Suit Code Descriptions.

CONTRACT
- ☐ 110 Insurance
- ☐ 120 Marine
- ☐ 130 Miller Act
- ☐ 140 Negotiable Instrument
- ☐ 150 Recovery of Overpayment & Enforcement of Judgment
- ☐ 151 Medicare Act
- ☐ 152 Recovery of Defaulted Student Loans (Excludes Veterans)
- ☐ 153 Recovery of Overpayment of Veteran's Benefits
- ☐ 160 Stockholders' Suits
- ☐ 190 Other Contract
- ☐ 195 Contract Product Liability
- ☐ 196 Franchise

REAL PROPERTY
- ☐ 210 Land Condemnation
- ☐ 220 Foreclosure
- ☐ 230 Rent Lease & Ejectment
- ☐ 240 Torts to Land
- ☐ 245 Tort Product Liability
- ☐ 290 All Other Real Property

TORTS

PERSONAL INJURY
- ☐ 310 Airplane
- ☐ 315 Airplane Product Liability
- ☐ 320 Assault, Libel & Slander
- ☐ 330 Federal Employers' Liability
- ☐ 340 Marine
- ☐ 345 Marine Product Liability
- ☐ 350 Motor Vehicle
- ☐ 355 Motor Vehicle Product Liability
- ☐ 360 Other Personal Injury
- ☐ 362 Personal Injury - Medical Malpractice

PERSONAL INJURY
- ☐ 365 Personal Injury - Product Liability
- ☐ 367 Health Care/ Pharmaceutical Personal Injury Product Liability
- ☐ 368 Asbestos Personal Injury Product Liability

PERSONAL PROPERTY
- ☐ 370 Other Fraud
- ☐ 371 Truth in Lending
- ☐ 380 Other Personal Property Damage
- ☐ 385 Property Damage Product Liability

CIVIL RIGHTS
- ☐ 440 Other Civil Rights
- ☐ 441 Voting
- ☐ 442 Employment
- ☐ 443 Housing/ Accommodations
- ☐ 445 Amer. w/Disabilities - Employment
- ☐ 446 Amer. w/Disabilities - Other
- ☐ 448 Education

PRISONER PETITIONS

Habeas Corpus:
- ☐ 463 Alien Detainee
- ☐ 510 Motions to Vacate Sentence
- ☐ 530 General
- ☐ 535 Death Penalty

Other:
- ☐ 540 Mandamus & Other
- ☐ 550 Civil Rights
- ☐ 555 Prison Condition
- ☐ 560 Civil Detainee - Conditions of Confinement

FORFEITURE/PENALTY
- ☐ 625 Drug Related Seizure of Property 21 USC 881
- ☐ 690 Other

LABOR
- ☐ 710 Fair Labor Standards Act
- ☐ 720 Labor/Management Relations
- ☐ 740 Railway Labor Act
- ☐ 751 Family and Medical Leave Act
- ☐ 790 Other Labor Litigation
- ☐ 791 Employee Retirement Income Security Act

IMMIGRATION
- ☐ 462 Naturalization Application
- ☐ 465 Other Immigration Actions

BANKRUPTCY
- ☐ 422 Appeal 28 USC 158
- ☐ 423 Withdrawal 28 USC 157

INTELLECTUAL PROPERTY RIGHTS
- ☐ 820 Copyrights
- ☐ 830 Patent
- ☐ 835 Patent - Abbreviated New Drug Application
- ☐ 840 Trademark
- ☐ 880 Defend Trade Secrets Act of 2016

SOCIAL SECURITY
- ☐ 861 HIA (1395ff)
- ☐ 862 Black Lung (923)
- ☐ 863 DIWC/DIWW (405(g))
- ☐ 864 SSID Title XVI
- ☐ 865 RSI (405(g))

FEDERAL TAX SUITS
- ☐ 870 Taxes (U.S. Plaintiff or Defendant)
- ☐ 871 IRS—Third Party 26 USC 7609

OTHER STATUTES
- ☐ 375 False Claims Act
- ☐ 376 Qui Tam (31 USC 3729(a))
- ☐ 400 State Reapportionment
- ☐ 410 Antitrust
- ☐ 430 Banks and Banking
- ☐ 450 Commerce
- ☐ 460 Deportation
- ☐ 470 Racketeer Influenced and Corrupt Organizations
- ☐ 480 Consumer Credit (15 USC 1681 or 1692)
- ☐ 485 Telephone Consumer Protection Act
- ☐ 490 Cable/Sat TV
- ☐ 850 Securities/Commodities/ Exchange
- ☒ 890 Other Statutory Actions
- ☐ 891 Agricultural Acts
- ☐ 893 Environmental Matters
- ☐ 895 Freedom of Information Act
- ☐ 896 Arbitration
- ☐ 899 Administrative Procedure Act/Review or Appeal of Agency Decision
- ☐ 950 Constitutionality of State Statutes

V. ORIGIN *(Place an "X" in One Box Only)*

☒ 1 Original Proceeding ☐ 2 Removed from State Court ☐ 3 Remanded from Appellate Court ☐ 4 Reinstated or Reopened ☐ 5 Transferred from Another District *(specify)* ☐ 6 Multidistrict Litigation - Transfer ☐ 8 Multidistrict Litigation - Direct File

VI. CAUSE OF ACTION

Cite the U.S. Civil Statute under which you are filing ***(Do not cite jurisdictional statutes unless diversity)***:
18 U.S.C. § 1030

Brief description of cause:
T-Mobile is violating the Computer Fraud and Abuse Act, and other laws, by knowingly accessing and scraping confidential AT&T customer data.

VII. REQUESTED IN COMPLAINT:

☐ CHECK IF THIS IS A **CLASS ACTION** UNDER RULE 23, F.R.Cv.P.

DEMAND $

CHECK YES only if demanded in complaint:

JURY DEMAND: ☒ Yes ☐ No

VIII. RELATED CASE(S) IF ANY

(See instructions): JUDGE _____ DOCKET NUMBER _____

DATE 11/26/2025

SIGNATURE OF ATTORNEY OF RECORD /s/ Timothy S. Durst

FOR OFFICE USE ONLY

RECEIPT # _____ AMOUNT _____ APPLYING IFP _____ JUDGE _____ MAG. JUDGE _____

INSTRUCTIONS FOR ATTORNEYS COMPLETING CIVIL COVER SHEET FORM JS 44

Authority For Civil Cover Sheet

The JS 44 civil cover sheet and the information contained herein neither replaces nor supplements the filings and service of pleading or other papers as required by law, except as provided by local rules of court. This form, approved by the Judicial Conference of the United States in September 1974, is required for the use of the Clerk of Court for the purpose of initiating the civil docket sheet. Consequently, a civil cover sheet is submitted to the Clerk of Court for each civil complaint filed. The attorney filing a case should complete the form as follows:

I.(a) Plaintiffs-Defendants. Enter names (last, first, middle initial) of plaintiff and defendant. If the plaintiff or defendant is a government agency, use only the full name or standard abbreviations. If the plaintiff or defendant is an official within a government agency, identify first the agency and then the official, giving both name and title.

(b) County of Residence. For each civil case filed, except U.S. plaintiff cases, enter the name of the county where the first listed plaintiff resides at the time of filing. In U.S. plaintiff cases, enter the name of the county in which the first listed defendant resides at the time of filing. (NOTE: In land condemnation cases, the county of residence of the "defendant" is the location of the tract of land involved.)

(c) Attorneys. Enter the firm name, address, telephone number, and attorney of record. If there are several attorneys, list them on an attachment, noting in this section "(see attachment)".

II. Jurisdiction. The basis of jurisdiction is set forth under Rule 8(a), F.R.Cv.P., which requires that jurisdictions be shown in pleadings. Place an "X" in one of the boxes. If there is more than one basis of jurisdiction, precedence is given in the order shown below.
United States plaintiff. (1) Jurisdiction based on 28 U.S.C. 1345 and 1348. Suits by agencies and officers of the United States are included here.
United States defendant. (2) When the plaintiff is suing the United States, its officers or agencies, place an "X" in this box.
Federal question. (3) This refers to suits under 28 U.S.C. 1331, where jurisdiction arises under the Constitution of the United States, an amendment to the Constitution, an act of Congress or a treaty of the United States. In cases where the U.S. is a party, the U.S. plaintiff or defendant code takes precedence, and box 1 or 2 should be marked.
Diversity of citizenship. (4) This refers to suits under 28 U.S.C. 1332, where parties are citizens of different states. When Box 4 is checked, the citizenship of the different parties must be checked. (See Section III below; **NOTE: federal question actions take precedence over diversity cases.**)

III. Residence (citizenship) of Principal Parties. This section of the JS 44 is to be completed if diversity of citizenship was indicated above. Mark this section for each principal party.

IV. Nature of Suit. Place an "X" in the appropriate box. If there are multiple nature of suit codes associated with the case, pick the nature of suit code that is most applicable. Click here for: Nature of Suit Code Descriptions.

V. Origin. Place an "X" in one of the seven boxes.
Original Proceedings. (1) Cases which originate in the United States district courts.
Removed from State Court. (2) Proceedings initiated in state courts may be removed to the district courts under Title 28 U.S.C., Section 1441.
Remanded from Appellate Court. (3) Check this box for cases remanded to the district court for further action. Use the date of remand as the filing date.
Reinstated or Reopened. (4) Check this box for cases reinstated or reopened in the district court. Use the reopening date as the filing date.
Transferred from Another District. (5) For cases transferred under Title 28 U.S.C. Section 1404(a). Do not use this for within district transfers or multidistrict litigation transfers.
Multidistrict Litigation – Transfer. (6) Check this box when a multidistrict case is transferred into the district under authority of Title 28 U.S.C. Section 1407.
Multidistrict Litigation – Direct File. (8) Check this box when a multidistrict case is filed in the same district as the Master MDL docket. **PLEASE NOTE THAT THERE IS NOT AN ORIGIN CODE 7.** Origin Code 7 was used for historical records and is no longer relevant due to changes in statute.

VI. Cause of Action. Report the civil statute directly related to the cause of action and give a brief description of the cause. **Do not cite jurisdictional statutes unless diversity.** Example: U.S. Civil Statute: 47 USC 553 Brief Description: Unauthorized reception of cable service.

VII. Requested in Complaint. Class Action. Place an "X" in this box if you are filing a class action under Rule 23, F.R.Cv.P.
Demand. In this space enter the actual dollar amount being demanded or indicate other demand, such as a preliminary injunction.
Jury Demand. Check the appropriate box to indicate whether or not a jury is being demanded.

VIII. Related Cases. This section of the JS 44 is used to reference related cases, if any. If a related case exists, whether pending or closed, insert the docket numbers and the corresponding judge names for such cases. A case is related to this filing if the case: 1) involves some or all of the same parties and is based on the same or similar claim; 2) involves the same property, transaction, or event; 3) involves substantially similar issues of law and fact; and/or 4) involves the same estate in a bankruptcy appeal.

Date and Attorney Signature. Date and sign the civil cover sheet.