UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF WASHINGTON
SEATTLE DIVISION

VEERA DARUWALLA, MICHAEL MARCH, and LAVICIEIA STURDIVANT, individually and on behalf of classes of similarly situated individuals,

Plaintiffs,

v.

T-MOBILE USA, INC.

Defendant.

Case No.:

CLASS ACTION COMPLAINT FOR:

(1) Violation of the California Consumer Privacy Act § 1798.150
(2) Negligence
(3) Negligence *Per Se*
(4) Unjust Enrichment
(5) Breach of Implied Contract
(6) Breach of Confidence
(7) Declaratory and Injunctive Relief

DEMAND FOR JURY TRIAL

Plaintiffs Veera Daruwalla, Michael March, and Lavicieia Sturdivant ("Plaintiffs"), individually and on behalf of classes of similarly situated individuals (defined below), bring this action against Defendant T-Mobile USA, Inc. ("T-Mobile" or "Defendant"). Plaintiffs make the following allegations based upon personal knowledge as to their own actions and upon information and belief as to all other matters and believe that reasonable discovery will provide additional evidentiary support for the allegations herein.

I. NATURE OF THE CASE

1. "Not all data breaches are created equal. None of them are good, but they do come in varying degrees of bad. And given how regularly they happen, it's understandable that you may have become inured to the news. Still, a T-Mobile breach that hackers claim involved the data of 100 million people deserves your attention…." WIRED Magazine, *The T-Mobile Data Breach is One You Can't Ignore,* August 16, 2021.

2. On the same day that article was printed, T-Mobile confirmed that hackers using the Twitter handle ***@und0xxed*** had in fact gained unauthorized access to T-Mobile data through T-Mobile servers (the "Data Breach").

3. According to the hackers, the stolen personal identifying information ("PII") includes customers' names, addresses, social security numbers, drivers license information, phone numbers, dates of birth, security PINs, phone numbers, and, for some customers, unique IMSI and IMEI numbers (embedded in customer mobile devices that identify the device and the SIM card that ties that customer's device to a telephone number)—all going back as far as the mid 1990s. The hackers also claim to have a database that includes credit card numbers with six digits of the cards obfuscated.

4. As the WIRED article points out: "[T]he apparent T-Mobile breach offers potential buyers a blend of data that could be used to great effect." "[H]aving [this PII] centralized streamlines the [identity theft] process for criminals…" And while it may be true

that "names and phone numbers are relatively easy to find … a database that ties those two together, along with identifying someone's carrier and fixed address, makes it much easier to convince someone to click on a link that advertises, say, a special offer or upgrade for T-Mobile customers. And to do so en masse."

5. Furthermore, "[b]ecause each IMEI number is tied to a specific customer's phone, knowing it could help in a so-called SIM-swap attack" which "could lead to account takeover concerns…since threat actors could gain access to two-factor authentication or one-time passwords tied to other accounts—such as email, banking, or any other account employing advanced authentication security feature—using a victim's phone number." In fact, a previous T-Mobile data breach disclosed in February of this year—one of many it has suffered in the last few years—was used specifically to execute a SIM-swap attack.[1]

6. According to the hackers, the Data Breach reportedly affects more than 100 million individuals, meaning that all or nearly all T-Mobile customers may have been impacted.[2] As of August 18, T-Mobile has conceded that its "preliminary investigation" indicates that at *least* 7.8 million current T-Mobile postpaid customer accounts were in the stolen files, as well as over 40 million records of former or prospective customers who had previously applied for credit with T-Mobile, 850,000 active prepaid customers, and some additional information from inactive prepaid accounts access through prepaid billing files. The investigation appears ongoing and therefore may reveal additional affected accounts.

---

[1] *See, e.g.*, Gatlan, Sergio, *T-Mobile discloses data breach after SIM swapping attacks,* Bleeping Computer, Feb. 26, 2021, available at https://www.bleepingcomputer.com/news/security/t-mobile-discloses-data-breach-after-sim-swapping-attacks/.

[2] T-Mobile US Inc. (2020). Form 10-K 2020 at 5. Retrieved from https://www.sec.gov/ix?doc=/Archives/edgar/data/0001283699/000128369921000039/tmus-20201231.htm.

7. But while T-Mobile has confirmed that a breach occurred, it has yet to provide any notice or instruction to its customers, other than that "communications will be issued shortly" recommending that all T-Mobile postpaid customers proactively change their PIN and take advantage of Account Takeover Protection capabilities. Unfortunately, it is too late: according to the hackers, they have already sold a first batch containing hundreds of thousands of records and are shopping the bulk of the stolen PII directly to buyers.

8. As the target of many data breaches in the past, T-Mobile knew its systems were vulnerable to attack. Yet it failed to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect its customers' personal information, yet again putting millions of customers at great risk of scams and identity theft. Its customers expected and deserved better from the second largest wireless provider in the country.

9. The customer PII disclosed in the Data Breach is protected by the California Consumer Privacy Act of 2018, Cal. Civ. Code § 1798.100 ("CCPA"), which gives rise to a cause of action when insufficient security results in a breach. Specifically, the CCPA gives rise to a claim where, as here, an individual's name in combination with a social security number or driver's license number are exfiltrated without authorization (among other things).[3]

10. In a private right of action, the CCPA also provides for statutory damages of between $100 and $750 per customer per violation or actual damages, whichever is greater. The appropriate amount of statutory damages is determined through examination of a number of factors, including the size of Defendant's assets and whether the Defendant has a record of weak data security.

[3] In other sections of the CCPA, "personal information" is defined more broadly as "information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household."

11. Finally, the CCPA provides that "[a]ny provision of a contract or agreement of any kind that purports to waive or limit in any way a consumer's rights under this title, including, but not limited to, any right to a remedy or means of enforcement, shall be deemed contrary to public policy and shall be void and unenforceable."

12. Plaintiffs now seek compensation under the CCPA and principles of common law negligence, unjust enrichment, breach of implied contract, and breach of confidence, for their damages and those of fellow class members. Plaintiffs also seek injunctive relief to ensure that T-Mobile cannot continue to put its customers at risk.

II. JURISDICTION AND VENUE

13. This Court has jurisdiction over this action under the Class Action Fairness Act ("CAFA"), 28 U.S.C. § 1332(d), because the aggregate amount in controversy exceeds $5,000,000, exclusive of interests and costs, there are more than 100 class members, and one or more members of the classes are residents of a different state than the Defendant. The Court also has supplemental jurisdiction over the state law claims under 28 U.S.C. § 1367.

14. This Court has personal jurisdiction over Defendant because it is headquartered in this District.

15. Venue is proper in this District pursuant to 28 U.S.C. §§ 1391(b) and (c) and 15 U.S.C. §§ and 22, as Defendant resides, transacts business, committed an illegal or tortious act, has an agent, and/or can be found in this District.

III. PARTIES

16. Plaintiff Veera Daruwalla is a resident of Kern County, California. As a current T-Mobile customer since at least 2018, Ms. Daruwalla believes her PII was accessed without authorization, exfiltrated, and/or stolen in the Data Breach.

17. Plaintiff Michael March is a resident of Chalmette, Louisiana and was a T-Mobile customer for approximately eight years before canceling his services due to privacy

DOCKET ALARM

Explore Litigation Insights

Docket Alarm provides insights to develop a more informed litigation strategy and the peace of mind of knowing you're on top of things.

Real-Time Litigation Alerts

Keep your litigation team up-to-date with **real-time alerts** and advanced team management tools built for the enterprise, all while greatly reducing PACER spend.

Our comprehensive service means we can handle Federal, State, and Administrative courts across the country.

Advanced Docket Research

With over 230 million records, Docket Alarm's cloud-native docket research platform finds what other services can't. Coverage includes Federal, State, plus PTAB, TTAB, ITC and NLRB decisions, all in one place.

Identify arguments that have been successful in the past with full text, pinpoint searching. Link to case law cited within any court document via Fastcase.

Analytics At Your Fingertips

Learn what happened the last time a particular judge, opposing counsel or company faced cases similar to yours.

Advanced out-of-the-box PTAB and TTAB analytics are always at your fingertips.

API

Docket Alarm offers a powerful API (application programming interface) to developers that want to integrate case filings into their apps.

LAW FIRMS
Build custom dashboards for your attorneys and clients with live data direct from the court.

Automate many repetitive legal tasks like conflict checks, document management, and marketing.

FINANCIAL INSTITUTIONS
Litigation and bankruptcy checks for companies and debtors.

E-DISCOVERY AND LEGAL VENDORS
Sync your system to PACER to automate legal marketing.