

**IN THE UNITED STATES DISTRICT COURT  
FOR THE WESTERN DISTRICT OF MISSOURI**

IN RE: T-MOBILE CUSTOMER DATA ) MDL No. 3019  
SECURITY BREACH LITIGATION )  
) Master Case No. 4:21-MD-03019-BCW  
)  
)  
)

**CONSOLIDATED CONSUMER CLASS ACTION COMPLAINT**

Norman E. Siegel  
**STUEVE SIEGEL HANSON LLP**  
460 Nichols Rd., Ste. 200  
Kansas City, MO 64112  
siegel@stuevesiegel.com

Cari Campen Laufenberg  
**KELLER ROHRBACK L.L.P.**  
1201 3rd Ave., Ste. 3200  
Seattle, WA 98101  
claufenberg@kellerrohrback.com

James J. Pizzirusso  
**HAUSFELD LLP**  
888 16th St. NW, Ste. 300  
Washington, DC 20006  
jpizzirusso@hausfeld.com

*Co-Lead Interim Class Counsel*

**TABLE OF CONTENTS**

INTRODUCTION ..... 1

JURISDICTION AND VENUE ..... 1

PLAINTIFFS ..... 2

STATEMENT OF FACTS ..... 36

CLASS ACTION ALLEGATIONS ..... 65

CLAIMS ON BEHALF OF THE NATIONWIDE CLASS ..... 71

CLAIMS ON BEHALF OF THE STATE SUBCLASSES ..... 91

REQUEST FOR RELIEF ..... 331

## INTRODUCTION

*“You can trust us to do the right thing with your data.”*

1. With over 100 million customers, T-Mobile is one of the largest consumer brands in the United States. It collects vast troves of personal information from its customers and prospective customers and profits from that data through its own marketing efforts and by selling sensitive consumer information to third parties. T-Mobile understood it had an enormous responsibility to protect the data it collected and assured consumers through its Privacy Policy that T-Mobile uses “administrative, technical, contractual, and physical safeguards designed to protect your data while it is under our control.” Its Privacy Center likewise assured consumers that “[w]ith T-Mobile, you don’t have to worry,” “[w]e’ve got your back,” and “you can trust us to do the right thing with your data.” But, as T-Mobile admitted, it completely failed to meet these obligations and protect sensitive consumer data. Instead, T-Mobile suffered one of the largest and most consequential data breaches in U.S. history, compromising the sensitive personal information of over 75 million consumers.

## JURISDICTION AND VENUE

2. This Court has subject matter jurisdiction pursuant to the Class Action Fairness Act of 2005, 28 U.S.C. § 1332(d)(2), because this is a class action in which the matter in controversy exceeds the sum of \$5,000,000, there are more than 100 proposed Class Members, and minimal diversity exists as Defendant is a citizen of States different from that of at least one Class member. This Court also has supplemental jurisdiction pursuant to 28 U.S.C. § 1367(a) because all claims alleged herein form part of the same case or controversy.

3. This Court has personal jurisdiction over T-Mobile because it is authorized to and regularly conducts business in the State of Missouri. T-Mobile sells, markets, and advertises its products and services to Plaintiffs and Class Members located in the State of Missouri and,

therefore, has sufficient minimum contacts to render the exercise of jurisdiction by this Court proper and necessary. Moreover, T-Mobile specifically requested the case be transferred to this District.

4. Venue is proper in this District pursuant to 28 U.S.C. § 1407 and the January 31, 2022, Transfer Order of the Judicial Panel on Multidistrict Litigation in MDL 3019 or, in the alternative, pursuant to 28 U.S.C. § 1391 because Defendant transacts business and may be found in this District.

### **DEFENDANT**

5. Defendants T-Mobile US, Inc. and its wholly-owned subsidiary T-Mobile USA, Inc. (“Defendant” or “T-Mobile”) are a telecommunications company that provides wireless voice, messaging, and data services along with mobile phones and accessories. T-Mobile is headquartered in Bellevue, Washington and Overland Park, Kansas in the Kansas City Metropolitan area, and is incorporated under the laws of the State of Delaware.

### **PLAINTIFFS**

6. Plaintiffs are individuals who, upon information and belief, had their personally-identifiable information (“PII”)<sup>1</sup> exfiltrated and compromised in the data breach announced by T-Mobile on August 16, 2021 (the “Data Breach”), and they bring this action on behalf of themselves and all those similarly situated both across the United States and within their State residence. The following allegations are made upon information and belief derived from, among other things, investigation of counsel, public sources, and the facts and circumstances as currently known. Because only T-Mobile (and the hackers) have knowledge of what information

---

<sup>1</sup> PII is information that is used to confirm an individual’s identity and can include an individual’s name, Social Security number, driver’s license number, phone number, financial information, and other identifying information unique to an individual. For T-Mobile, this information also includes unique technical identifiers tethered to customers’ mobile phones.

was compromised for each individual Plaintiff, Plaintiffs reserve their right to supplement their allegations with additional facts and injuries as they are discovered.

7. Plaintiffs place significant value in the security of their PII. Plaintiffs entrusted their sensitive PII to T-Mobile with the understanding that T-Mobile would keep their information secure and employ reasonable and adequate security measures to ensure that it would not be compromised. If Plaintiffs had known of T-Mobile's lax security practices with respect to Plaintiffs' PII, they would not have done business with T-Mobile, would not have applied for T-Mobile's services or purchased its products, would not have opened, used, or continued to use T-Mobile's cell phone and other telecommunications-related services at the applicable rates and on the applicable terms, or would have paid less because of the diminished value of T-Mobile's services.

#### **ALABAMA**

8. Plaintiff Dana Snider is a resident of the State of Alabama and is a current customer of T-Mobile. Plaintiff Snider was notified by a third-party monitoring company that her PII was located on the dark web as a result of the T-Mobile Data Breach. In addition, as a result of the breach, Plaintiff Snider spent time and effort researching the breach and monitoring her accounts for fraudulent activity. Given the highly-sensitive nature of the information stolen, and its subsequent dissemination to unauthorized parties, Plaintiff Snider has already suffered injury and remains at a substantial and imminent risk of future harm.

#### **ARIZONA**

9. Plaintiff Tonya Bauer is a resident of the State of Arizona and is a current customer of T-Mobile. Plaintiff Bauer was notified by T-Mobile that her PII was compromised in the T-Mobile Data Breach. As a result of the breach, Plaintiff Bauer has suffered fraud in the form of unauthorized attempted bank transfers. As a result of this fraud, Plaintiff Bauer spent

# 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.