1 **AYLSTOCK, WITKIN, KREIS &**

2 **OVERHOLTZ, PLLC**
S. MARY LIU, ESQ. (SBN # 282884)

3 17 East Main St, Suite 200
Pensacola, FL32502

4 Tel: 850-202-1010
Fax: 760-304-8933

5 Email: mliu@awkolaw.com

6

7 **BRADLEY/GROMBACHER, LLP**
Marcus J. Bradley, Esq. (SBN 174156)

8 Kiley L. Grombacher, Esq. (SBN 245960)
Lirit A. King, Esq. (SBN 252521)

9 31365 Oak Crest Drive, Suite 240
Westlake Village, California 91361

10 Telephone: (805) 270-7100

11 Facsimile: (805) 270-7589
E-Mail: mbradley@bradleygrombacher.com

12   kgrombacher@bradleygrombacher.com

13   lking@bradleygrombacher.com

14

15 Attorneys for Plaintiff

16   **UNITED STATES DISTRICT COURT**

17   **CENTRAL DISTRICT OF CALIFORNIA**

18 JENNIFER BAUGHMAN, an   **CASE NO:**
individual, and on behalf of classes of

19 similarly situated individuals,   **CLASS ACTION**

20   Plaintiff,   **COMPLAINT FOR:**

21   1. **NEGLIGENCE;**
v.

22   2.   **UNJUST ENRICHMENT;**

23 T-Mobile US, Inc.,
                                               3. **BREACH OF EXPRESS**

24   Defendant.   **CONTRACT;**

25   4. **BREACH OF IMPLIED**
                                                  CONTRACT; AND

26   5. **INVASION OF PRIVACY.**

27   Demand for a jury trial

28

Plaintiff Jennifer Baughman ("Plaintiff") brings this Class Action Complaint against T-Mobile US, Inc. ("Defendant"), in her individual capacity and on behalf of all others similarly situated, and alleges, upon personal knowledge as to her own actions and her counsels' investigations, and upon information and belief as to all other matters, as follows:

INTRODUCTION

1.   This is a class action for damages with respect to Defendant T-Mobile US, Inc. and its failure to exercise reasonable care in securing sensitive personal information including without limitation, unencrypted and unredacted name, contact and demographic information, and date of birth (collectively, "personal identifiable information" or "PII").

2.   Plaintiff seeks damages for herself and other similarly situated current and former student loan borrowers ("borrowers"), or any other person(s) impacted in the data breach at issue ("Class Members"), as well as other equitable relief, including, without limitation, injunctive relief designed to protect the very sensitive information of Plaintiff and other Class Members.

3.   On or about January 20, 2023, Defendant notified Plaintiff and Class Members about a widespread data breach involving sensitive PII. The number of individuals affected has been estimated to impact 37 million customers by Defendant, however, because Defendant is one of the largest technology companies, the breach could have involved hundreds of millions of users. Defendant discovered that files on its network were accessed and acquired by the unauthorized actor (the "Data Breach").

4.   Plaintiff and the Class Members in this action were, upon information and belief, current and former Defendant users with their PII on Defendant's system. Upon information and belief, the first that Plaintiff and the Class Members learned of the Data Breach was when they saw news reports of the Data Breach on approximately January 20, 2023.

5.   The Data Breach affected individuals whose information was stored on Defendant's servers in multiple states.

6.   In this era of frequent data security attacks and data breaches, particularly in the technology industry, Defendant's failures leading to the Data Breach are particularly egregious, as this Data Breach was highly foreseeable.

7.   Upon information and belief, Plaintiff's and Class Members' PII was unencrypted and unredacted PII and was compromised due to Defendant's negligent and/or careless acts and omissions.

8.   As a result of the Data Breach, Plaintiff and the Class Members are at an imminent risk of identity theft.

9.   Plaintiff and Class Members have suffered numerous actual and concrete injuries as a direct result of the Data Breach, including: (a) invasion of privacy; (b) financial costs incurred mitigating the materialized risk and imminent threat of identity theft; (c) loss of time and loss of productivity incurred mitigating the materialized risk and imminent threat of identity theft; (d) financial costs incurred due to actual identity theft; (e) loss of time incurred due to actual identity theft; (f) loss of time heeding Defendant's warnings and following its instructions in the Notice Letter; (g) the loss of benefit of the bargain (price premium damages), to the extent Class Members paid Defendant for services; (h) deprivation of value of their PII; and (i) the continued risk to their Sensitive Information, which remains in the possession of Defendant, and which is subject to further breaches, so long as Defendant fails to undertake appropriate and adequate measures to protect Plaintiff's and Class Members' Sensitive Information.

10.   Plaintiff seeks to remedy these harms, and to prevent the future occurrence of an additional data breach, on behalf of themselves and all similarly situated persons whose PII was compromised as a result of the Data Breach. Plaintiff seeks remedies including, but not limited to, compensatory damages, reimbursement for loss of time, reimbursement of opportunity costs, out-of-pocket costs, price

1 premium damages, and injunctive relief including improvements to Defendant's data

2 security systems and protocols, future annual audits, and adequate credit monitoring

3 services funded by the Defendant.

PARTIES

5 11.   Plaintiff Jennifer Baughman is a resident and citizen of California,

6 residing at all relevant times in Los Angeles county.

7 12.   Defendants T-Mobile US, Inc. and its wholly-owned subsidiary T-

8 Mobile USA, Inc. ("Defendant" or "T-Mobile") are a telecommunications company

9 that provides wireless voice, messaging, and data services along with mobile phones

10 and accessories. T-Mobile is headquartered in Bellevue, Washington and Overland

11 Park, Kansas in the Kansas City Metropolitan area, and is incorporated under the

12 laws of the State of Delaware

13 13.   All of Plaintiff's claims stated herein are asserted against Defendant and

14 any of its owners, predecessors, successors, subsidiaries, agents and/or assigns.

JURISDICTION AND VENUE

16 14.   This Court has subject matter jurisdiction of this action pursuant to 28

17 U.S.C. § 1332, the Class Action Fairness Act of 2005 because: (i) there are 100 or

18 more class members, (ii) there is an aggregate amount in controversy exceeding

19 $5,000,000, exclusive of interest and costs, and (iii) there is minimal diversity

20 because at least one Plaintiff (FL) and Defendant are citizens of different states. This

21 Court has supplemental jurisdiction over any state law claims pursuant to 28 U.S.C.

22 § 1367.

23 15.   This Court has personal jurisdiction over T-Mobile because it is

24 authorized to and regularly conducts business in the State of California. T-Mobile

25 sells, markets, and advertises its products and services to Plaintiffs and Class

26 Members located in the State of California and, therefore, has sufficient minimum

27 contacts to render the exercise of jurisdiction by this Court proper and necessary.

28 16.   Pursuant to 28 U.S.C. § 1391, this Court is the proper venue for this

1   action because a substantial part of the events, omissions, and acts giving rise to the

2   claims herein occurred in this District: Class members affected by the breach reside

3   in this District and Defendant employs numerous people in this District.

FACTUAL ALLEGATIONS

4

5   17.   Defendant operates its business nationwide offering various types of

6   technological products and services.

7   18.   Plaintiff and the Class Members, as current or former T-Mobile users,

8   reasonably relied (directly or indirectly) on this sophisticated technology company to

9   keep their sensitive PII confidential; to maintain its system security; to use this

10 information for business purposes only; and to make only authorized disclosures of

11 their PII. Borrowers, in general, demand security to safeguard their PII, especially

12 when financial information and other sensitive PII is involved.

13   19.   On or about January 20, 2023, Defendant made an announcement about

14 a widespread data breach of its computer network involving the sensitive personally

15 identifiable information of consumers.

16   20.   According to news reports: "A 'bad actor' stole personal information

17 from approximately 37 million T-Mobile customers in a November data breach."[1]

18   21.   In a filing with the Securities and Exchange Committee: "T-Mobile said

19 the hack was discovered on Jan. 5. The unidentified hacker (or hackers) obtained data

20 starting around Nov. 25 through a single Application Programming Interface, the

21 company said."[2]

22   22.   Plaintiff and Class Members in this action were, upon information and

23 belief, current and former T-Mobile users whose PII was utilized by Defendant for

24 purposes of providing products and services. Plaintiff and Class Members first

25 learned of the Data Breach when they saw news reports of the Data Breach on or

26 about January 20, 2023.

27

28

[1] https://www.usatoday.com/story/tech/2023/01/20/tmobile-data-hack-37-million-customers/11088603002/

[2] *Id*.

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.