UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF WASHINGTON

STEPHANIE ESPANOZA, JONATHAN MORALES and ALEX PYGIN, individually and on behalf of all others similarly situated, Plaintiffs, v. T-MOBILE USA, INC., Defendant.	Case No. **CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

Plaintiffs Stephanie Espanoza, Jonathan Morales and Alex Pygin ("Plaintiffs") bring this Class Action Complaint against Defendant T-Mobile USA, Inc. ("T-Mobile" or "Defendant") as individuals and on behalf of all others similarly situated, and allege, upon personal knowledge as to their own actions, their counsel's investigations, and facts that are a matter of public record, and upon information and belief as to all other matters, as follows:

I. NATURE OF THE ACTION

1. This class action arises out of the recent cyberattack and data breach that was perpetrated against Defendant T-Mobile, a national telecommunications company that provides mobile telephone services to customers throughout the United States (the "Data Breach"). The Data Breach resulted in unauthorized access and exfiltration of highly sensitive and personal information (the "Private Information").

2. As a result of the Data Breach, Plaintiffs and approximately 40 million former or prospective customers who applied for credit with T-Mobile, 7.8 million current postpaid customers, and 850,000 active prepaid customers (the "Class Members")[1] suffered present injury and damages in the form of identity theft, out-of-pocket expenses and the value of the time reasonably incurred to remedy or mitigate the effects of the unauthorized access, exfiltration, and subsequent criminal misuse of their sensitive and highly personal information.

3. The Private Information compromised in the Data Breach includes names, phone numbers, drivers' licenses, government identification numbers, Social Security numbers, dates of birth, and T-Mobile account PINs. [2]

4. Plaintiffs bring this class action lawsuit on behalf of those similarly situated to address Defendant's inadequate safeguarding of Class Members' Private Information that it collected and maintained.

5. Defendant maintained the Private Information in a reckless manner. In particular, the Private Information was maintained on Defendant's computer system and network in a condition vulnerable to cyberattacks.

6. The mechanism of the cyberattack and potential for improper disclosure of Plaintiffs' and Class Members' Private Information was a known risk to Defendant, and thus Defendant was on notice that failing to take steps necessary to secure the Private Information from the risk of a ransomware attack.

7. Plaintiffs' and Class Members' identities are now at considerable risk because of Defendant's negligent conduct since the Private Information that T-Mobile collected and maintained is now in the hands of data thieves.

[1] *See T-Mobile Shares Additional Information Regarding Ongoing Cyberattack Investigation*, T-Mobile (Aug. 17, 2021), https://www.t-mobile.com/news/network/additional-information-regarding-2021-cyberattack-investigation (last visited Aug. 19, 2021).

[2] *Id*.

8. Armed with the Private Information accessed in the Data Breach, data thieves can commit a variety of crimes, including but not limited to fraudulently applying for unemployment benefits, opening new financial accounts in Class Members' names, taking out loans in Class Members' names, using Class Members' information to obtain government benefits (including unemployment or COVID relief benefits), filing fraudulent tax returns using Class Members' information, obtaining driver's licenses in Class Members' names but with another person's photograph and providing false information to police during an arrest.

9. Plaintiffs' and Class Members' Private Information was compromised due to Defendant's negligent and/or careless acts and omissions and its failure to adequately protect the Private Information of its current, former, and prospective clients.

10. As a result of the Data Breach, Plaintiffs and Class Members are exposed to a heightened present and imminent risk of fraud and identity theft. As a result of Defendant's actions and inactions, as set forth herein, Plaintiffs and Class Members must now and in the future closely monitor their financial accounts and information to guard against identity theft, among other issues.

11. Plaintiffs and Class Members have and may in the future incur actual monetary costs, including but not limited to the cost of purchasing credit monitoring services, credit freezes, credit reports or other protective measures to deter and detect identity theft.

12. Plaintiffs and Class Members have and may in the future expend time spent mitigating the effects of the Data Breach, including time spent dealing with actual or attempted fraud and identity theft.

13. By their Complaint, Plaintiffs seek to remedy these harms on behalf of themselves and all similarly situated individuals whose Private Information was accessed during the Data Breach.

14. Accordingly, Plaintiffs bring this action on behalf of all persons whose Private Information was compromised as a result of Defendant's negligence and failure to: (i) adequately protect its customer's Private Information, (ii) warn its current, former, and

potential customers of their inadequate information security practices, and (iii) effectively monitor their data systems for security vulnerabilities and incidents. Defendant's conduct amounts to negligence and violates federal and state statutes.

15. Plaintiffs seek remedies including, but not limited to, compensatory damages, reimbursement of out-of-pocket costs, and injunctive relief including improvements to Defendant's data security systems, future annual audits, and adequate credit monitoring services funded by Defendant.

II. PARTIES

16. Plaintiff Stephanie Espanoza is a citizen of California residing in Los Angeles, California.

17. Plaintiff Jonathan Morales is a citizen of California residing in Sacramento, California.

18. Plaintiff Alex Pygin is a citizen of California residing in Irvine, California.

19. Defendant T-Mobile is a for-profit company incorporated in Delaware with its principal place of business in the State of Washington at 12920 SE 38th St, Bellevue, Washington 98006.

III. JURISDICTION AND VENUE

20. This Court has subject matter jurisdiction over this action under 28 U.S.C. § 1332(d) because this is a class action wherein the amount in controversy exceeds the sum or value of $5,000,000, exclusive of interest and costs, there are more than 100 members in the proposed class, and at least one member of the class is a citizen of a state different from Defendant.

21. This Court has personal jurisdiction over Defendant because Defendant has its principal place of business is located in the State of Washington.

22. Venue is proper in this Court pursuant to 28 U.S.C. § 1391 because a substantial part of the events or omissions giving rise to these claims occurred in, were directed to, and/or

emanated from this District. Defendant resides within this judicial district and a substantial part of the events giving rise to the claims alleged herein occurred within this judicial district.

IV. FACTUAL ALLEGATIONS

A. Defendant's Business

23. Defendant is a national telecommunications company that provides mobile communication services, among other products and services, throughout the United States and around the globe.

24. In 2019 alone, T-Mobile claims to have increased its customer base by 7 million and had revenues totaling $45 billion. [3]

25. According to Defendant, as of the second quarter of 2021, T-Mobile had 104.8 million customers, making it one of the largest telecommunications providers in the United States and in the world. [4]

26. Upon information and belief, in the ordinary course of doing business, Defendant collects sensitive Private Information from customers and potential customers such as:

- Name;
- Address;
- Phone number;
- Driver's license number;
- Social Security number;
- Financial information;
- Government identification number; and
- Date of birth.

[3] *See Our Story*, T-Mobile, https://www.t-mobile.com/our-story (last visited Aug. 19, 2021).
[4] *See Investor Factbook*, T-Mobile, https://s24.q4cdn.com/400059132/files/doc_financials/2021/q2/NG_TMUS-06_30_2021-EX-99.2.pdf, at p. 6 (last visited Aug. 19, 2021).

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.