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

RYAN PHILPOT on behalf of himself and all others similarly situated, Plaintiff, v. T-MOBILE USA, INC. Defendant.	)	Case No. _____

Prologue

Customers trust us with their private information and we safeguard it with the utmost concern. A recent cybersecurity incident put some of that data in harm's way, and we apologize for that. We take this very seriously, and we strive for transparency in the status of our investigation and what we're doing to help protect you.[1]

CLASS ACTION COMPLAINT

Plaintiff Ryan Philpot ("Plaintiff"), brings this Class Action Complaint, on behalf of himself and all others similarly situated, against Defendant**,** T-Mobile USA, Inc. ("T-Mobile" or "Defendant"), alleging as follows based upon information and belief and investigation of counsel, except as to the allegations specifically pertaining to him, which is based on personal knowledge:

NATURE OF THE CASE

1. Plaintiff brings this class action against T-Mobile for T-Mobile's failure to properly secure and safeguard highly-valuable, protected personally identifiable information, including without limitations, social security numbers, phone numbers, names, physical addresses, unique IMEI numbers (International Mobile Equipment Identity – a 15 digit number unique to each

[1] https://www.t-mobile.com/brand/data-breach-2021(last accessed December 8, 2021).

mobile device), and driver licenses information (collectively, "PII"), failure to comply with industry standards to protect information systems that contain PII, and failure to provide adequate notice to Plaintiff and other members of the Class that their PII had been accessed and compromised. Plaintiff seeks, among other things, damages, orders requiring T-Mobile to fully and accurately disclose the nature of the PII and other information that has been compromised and to adopt reasonably sufficient security practices and safeguards to protect Plaintiff's and the Class Members' PII and to prevent incidents like this disclosure in the future. Plaintiff further seeks an order requiring T-Mobile to provide identity theft protective services to Plaintiff and members of the Class for their lifetimes, as Plaintiff and members of the Class are, and will continue to be at an increased risk of identity theft due to the disclosure of their PII as a result of the conduct of T-Mobile described herein.

2. T-Mobile is a mobile telecommunication company that provides mobile telephone service, internet, banking, and television services and products to individuals and businesses across the United States.

3. To obtain T-Mobile's services, T-Mobile requires users to create an account and/or enter into a contract with T-Mobile for a set period of time. During the account creation process, Plaintiff and other users are required to provide their PII to T-Mobile.

4. On or about August 15, 2021, T-Mobile's data, which purports to include the PII of over 100 million T-Mobile users, was put on a forum for sale for 6 bitcoin, or approximately $270,000. T-Mobile announced that it was continuing to investigate the breach but has confirmed that the breach has occurred, and the PII is in the hands of bad actors (the "Data Breach").

5. The Data Breach was a direct and proximate result of T-Mobile's failure to implement and follow basic security procedures and as a direct result of this failure Plaintiff's and

Class Members' PII is now in the hands of criminals. Plaintiff and members of the Class now face a substantially increased risk of identity theft, both currently and for the indefinite future, at least in part because their PII will now be offered and sold to identity thieves in an aggregated format, lending itself for ease of use in widespread phishing email schemes, identity theft and other harms caused by the disclosure of their PII. Consequently, Plaintiff and members of the Class have had to spend, and will continue to spend, significant time and money in the future to protect themselves due to T-Mobile's actions.

6. Plaintiff, on behalf of himself and all others similarly situated, bring claims for negligence, negligence *per se*, and declaratory judgment. Plaintiff seeks damages and injunctive relief, including and requiring T-Mobile to adopt reasonably sufficient practices to safeguard PII that remains in T-Mobile's custody in order to prevent incidents like the Data Breach from reoccurring in the future.

PARTIES

7. Plaintiff is a citizen and resident of the State of Missouri. At all times relevant to this Complaint, Plaintiff was a customer of T-Mobile. Plaintiff's PII was disclosed without authorization to unknown third parties as a result of T-Mobile's Data Breach.

8. Since the announcement of the Data Breach, Plaintiff has been required to spend valuable time monitoring his various accounts in an effort to detect and prevent any misuses of his PII – time which he would not have had to expend but for the Data Breach.

9. As a result of the Data Breach, Plaintiff has been and will continue to be at heightened risk for fraud and identity theft, and their attendant damages for years to come. Such risk is certainly impending and is not speculative, given that information from the Data Breach is already being offered for sale on the dark web.

10. Defendant T-Mobile, Inc. is a Delaware Corporation with its principal place of business located at 3618 Factoria Boulevard SE, Bellevue, Washington.

JURISDICTION AND VENUE

11. This Court has jurisdiction over this action pursuant to 28 U.S.C. § 1332(d)(2)(A), as modified by the Class Action Fairness Act of 2005, because Plaintiff and at least one member of the Class, as defined below, are citizens of a different state than Defendant, there are more than 100 members of each of the Class, and the aggregate amount in controversy exceeds $5,000,000 exclusive of interests and costs.

12. The Court has personal jurisdiction over Defendant because at all relevant times it has engaged in substantial business activities in Missouri. Defendant has, at all relevant times, transacted, solicited, and conducted business in Missouri through its employees, agents, and/or sales representatives, and derived substantial revenue from such business in Missouri.

13. Venue is proper in this district pursuant to 28 U.S.C. § 1391(b)(2) because a substantial part of the events or omissions giving rise to the claim occurred in this district.

FACTUAL BACKGROUND

T-Mobile

14. T-Mobile claims that it "deliver[s] outstanding wireless experiences" where "[p]eople come first."[2]

15. T-Mobile proclaims that it "is the leader in 5G coverage and speed. And according to competitive testing by umlaut, we're also the most reliable. No one else covers more people with the fastest and most reliable 5G."[3]

[2] https://www.t-mobile.com/about-us
[3] https://www.t-mobile.com/coverage/4g-lte-5g-networks?coverageMap=verizon

16. T-Mobile indicates that its merger with Sprint "strengthen[ed] our commitment to build out the best network around. Now, we're continuing to unite the power of our networks to bring 5G to more and more Americans every day."[4] It claims to have broader coverage, faster speeds, and greater signal strength.

17. T-Mobile offers wireless plans, phones, and devices[5], business phones[6], pre-paid plans[7], television through YouTube TV[8], banking services through T-Mobile MONEY[9], and internet services[10].

18. According to its 2020 Annual Report, T-Mobile services over 102.1 million mobile users, a significant increase from 67.9 million users in 2019.[11]

19. T-Mobile's users are entitled to security of their PII. As a vendor storing sensitive data, T-Mobile has a duty to ensure that such private, sensitive information is secure and is not disclosed or disseminated to unauthorized third parties.

The T-Mobile Data Breach

20. On August 15, 2021, T-Mobile stated that it was investigating a post on an online forum that claims to be selling a large amount of its consumers data, including PII.[12]

21. Motherboard reviewed a sample of the data for sale and confirmed that it appeared authentic.[13] The bad actor told Motherboard that the data comprised of over 100 million T-Mobile users, and that it included PII.[14]

---

[4] *Id.*
[5] https://www.t-mobile.com/
[6] https://www.t-mobile.com/business
[7] https://prepaid.t-mobile.com/home
[8] https://www.t-mobile.com/tvision
[9] https://www.t-mobilemoney.com/en/home.html
[10] https://www.t-mobile.com/isp
[11] https://s24.q4cdn.com/400059132/files/doc_financials/2020/ar/TMUS-2020-Annual-Report.pdf
[12] https://www.theverge.com/2021/8/15/22626270/t-mobile-investigating-report-customer-data-breach
[13] *Id.*
[14] *Id.*

22. The PII was listed on the forum for sale for a price of 6 bitcoin, or approximately $270,000, which included a subset of the data containing 30 million social security numbers and drivers licenses.[15] The bad actor indicated that the rest of the data was being sold privately.

23. Although it appears that T-Mobile fixed their exploited server and was able to remove the bad actor from having access, the bad actor indicated that the data was already downloaded locally.[16]

24. On August 16, 2021, T-Mobile released a "Cybersecurity Incident Update" indicating that "[w]e have determined that unauthorized access to some T-Mobile data occurred, however we have not yet determined that there is any personal customer data involved. We are confident that the entry point used to gain access has been closed, and we are continuing our deep technical review of the situation across our systems to identify the nature of any data that was illegally accessed."[17]

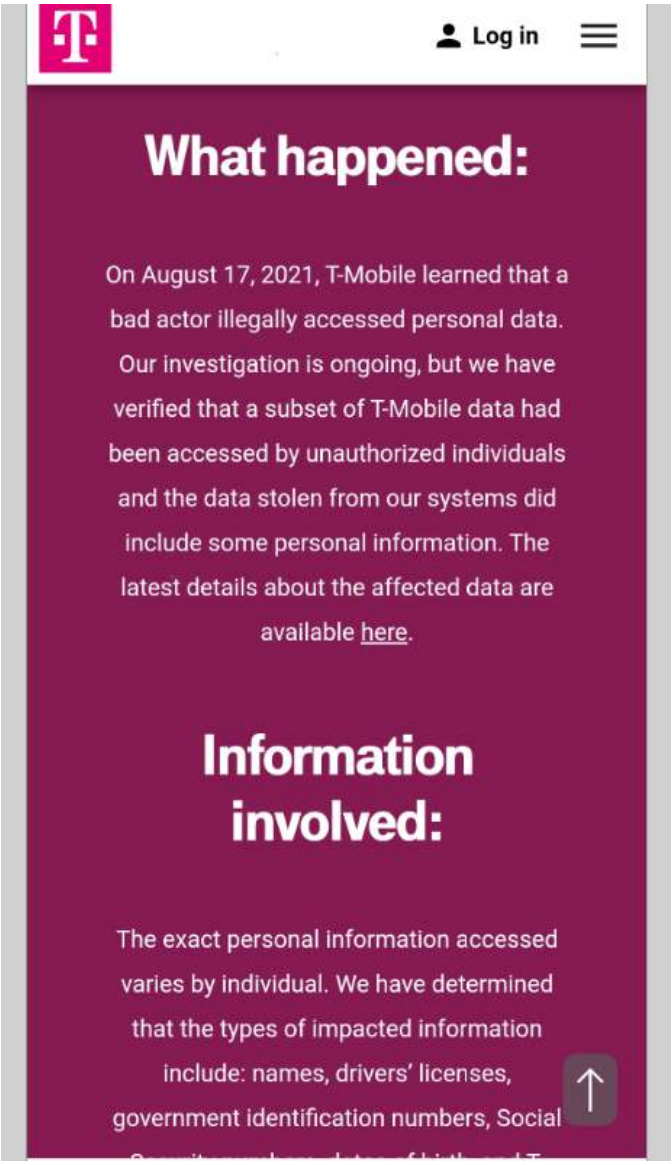
25. On August 17, 2021, T-Mobile released an update confirming that "[w]hile our investigation is still underway and we continue to learn additional details, we have now been able to confirm that the data stolen from our systems did include some personal information."[18] "Some of the data accessed did include customers' first and last names, date of birth, SSN, and driver's license/ID information for a subset of current and former postpay customers and prospective T-Mobile customers."[19]

26. In its August 17 release, T-Mobile indicated that "approximately 7.8 million current T-Mobile postpaid customer accounts' information appears to be contained in the stolen files, as

[15] *Id.*
[16] *Id.*
[17] https://www.t-mobile.com/news/network/cybersecurity-incident-update-august-2021
[18] https://www.t-mobile.com/news/network/additional-information-regarding-2021-cyberattack-investigation
[19] *Id.*

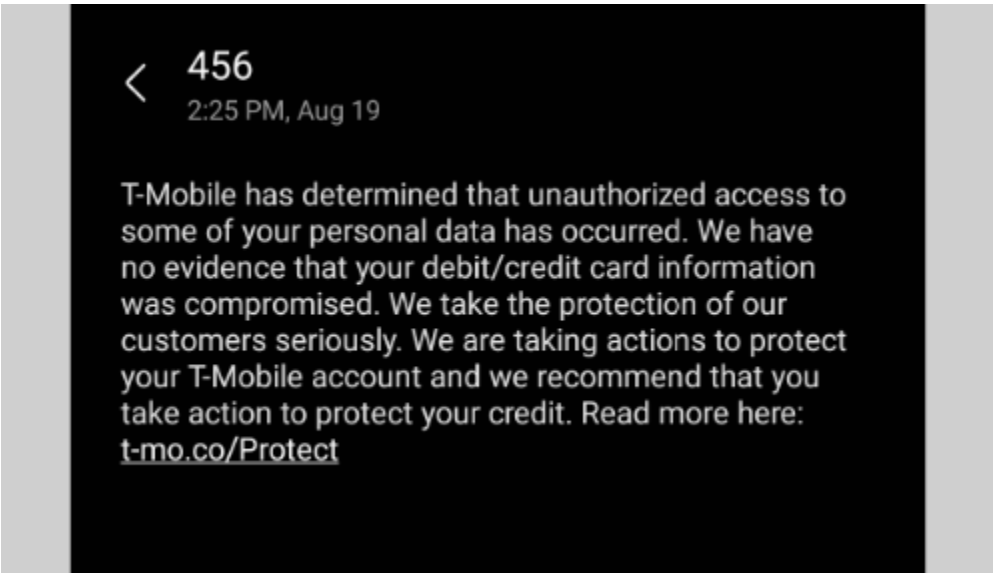
well as just over 40 million records of former or prospective customers who had previously applied for credit with T-Mobile."[20]

27. On August 19, 2021 T-Mobile notified its customers that a data breach had occurred and that personal data had been stolen by certain unauthorized individuals. T-Mobile acknowledged that the information that was stolen included names, drivers' licenses, social security numbers, drivers' licenses, government identification numbers.



[20] *Id.*

28. T-Mobile also notified its customers via text message that customers' personal data had been accessed and recommended that their customers take action to protect their credit.



29. On August 20, 2021, T-Mobile released an additional update indicating that, although the investigation is ongoing, there were confirmed an additional 5.3 million current users compromised, and an additional 667,000 former users compromised.[21]

T-Mobile Obtains, Collects, and Stores Plaintiff's and Class Members' PII

30. In the ordinary course of doing business with T-Mobile, users like Plaintiff and members of the Class are regularly required to provide their sensitive, personal and private protected information in order to register and use Defendant's services.

31. By obtaining, collecting, using, and deriving a benefit from Plaintiff's and Class Members' PII, T-Mobile assumed legal and equitable duties and knew or should have known that it was responsible for protecting Plaintiff's and Class Members' PII from disclosure.

32. Plaintiff and members of the Class reasonably expect that service providers such as Defendant will use the utmost care to keep this information confidential and securely maintained,

[21] *Id.*

to use this information for business purposes only, and to make only authorized disclosures of this information.

33. T-Mobile acknowledges that it has a duty to provide protection to this sensitive and personal information and claims that it will protect this data from being distributed. For example, T-Mobile states to its users that it offers the "privacy you deserve" and that "[w]ith T-Mobile, you don't have to worry."[22] T-Mobile proclaims that its "privacy principles mean you can trust us to do the right thing with your data" and that it will "provide tools to help keep you protected."[23]

34. T-Mobile continues that it "got your back" and are "always working to protect you and your family and keep your data secure."[24] "You trust T-Mobile to connect you to the world every day, and we're working hard to earn a place in your heart. A big part of that is maintaining your privacy. We believe you deserve transparency, education, choice, protection, and simplicity. Our goal is to help you take action to protect your privacy."[25]

35. Despite Defendant's commitment to protecting personal information, T-Mobile failed to prioritize data and cyber security by adopting reasonable data and cyber security measures to prevent and detect the unauthorized access to Plaintiff's and Class Members' PII.

36. Had T-Mobile remedied the deficiencies in its information storage and security systems, followed industry guidelines, and adopted security measures recommended by experts in the field, T-Mobile could have prevented intrusion into its information storage and security systems and, ultimately, the theft of Plaintiff's and Class Members' confidential PII.

[22] https://www.t-mobile.com/privacy-center
[23] *Id.*
[24] *Id.*
[25] https://www.t-mobile.com/privacy-center/our-practices/privacy-policy

The Value of Private Information and Effects of Unauthorized Disclosure

37. T-Mobile was well aware that the protected PII it acquires is highly sensitive and of significant value to those who would use it for wrongful purposes.

38. PII is a valuable commodity to identity thieves, particularly when it is aggregated in large numbers. As the FTC recognizes, identity thieves can use this information to commit an array of crimes including identity theft, and medical and financial fraud.[26] Indeed, a robust "cyber black market" exists in which criminals openly post stolen PII and other protected financial information on multiple underground Internet websites, commonly referred to as the "dark web."

39. PII is valued on the dark web at approximately $1 per line of information.[27] Social security number, birth date, and full name can sell for $60 to $80 as a bundle on the dark web.[28]

40. The ramifications of T-Mobile's failure to keep Plaintiff's and Class Members' PII secure are long lasting and severe. Once PII is stolen, fraudulent use of that information and damage to victims may continue for years.

41. Further, criminals often trade stolen PII on the "cyber black market" for years following a breach. Cybercriminals can also post stolen PII on the internet, thereby making such information publicly available.

42. T-Mobile knew, or should have known, the importance of safeguarding the PII entrusted to it and of the foreseeable consequences if its data security systems were breached. T-Mobile failed, however, to take adequate cyber security measures to prevent the Data Breach from occurring.

[26] https://www.consumer.ftc.gov/articles/0271-warning-signs-identity-theft
[27] https://www.pacetechnical.com/much-identity-worth-black-market/#:~:text=Personally%20identifiable%20information%20is%20sold,at%20a%20fast%20food%20joint.
[28] https://www.pcmag.com/news/heres-how-much-your-identity-goes-for-on-the-dark-web

FTC Guidelines

43. T-Mobile is prohibited by the Federal Trade Commission Act, 15 U.S.C. § 45 ("FTC Act") from engaging in "unfair or deceptive acts or practices in or affecting commerce." The Federal Trade Commission ("FTC") has concluded that a company's failure to maintain reasonable and appropriate data security for consumers' sensitive personal information is an "unfair practice" in violation of the FTC Act.

44. The FTC has promulgated numerous guidelines for businesses that highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.[29]

45. The FTC provided cybersecurity guidelines for businesses, advising that businesses should protect personal customer information, properly dispose of personal information that is no longer needed, encrypt information stored on networks, understand their network's vulnerabilities, and implement policies to correct any security problems.[30]

46. The FTC further recommends that companies not maintain PII longer than is needed for authorization of a transaction; limit access to private data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.[31]

47. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an

[29] https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf
[30] https://www.ftc.gov/system/files/documents/plain-language/pdf-0136proteting-personal-information.pdf.
[31] *Id.*

unfair act or practice prohibited by Section 5 of the FTC Act. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

48. T-Mobile failed to properly implement basic data security practices. T-Mobile's failure to employ reasonable and appropriate measures to protect against unauthorized access to consumer PII constitutes an unfair act of practice prohibited by Section 5 of the FTC Act.

49. T-Mobile was at all times fully aware of its obligations to protect the PII of consumers because of its business model of collecting PII and storing payment information. T-Mobile was also aware of the significant repercussions that would result from its failure to do so.

Plaintiff's and Class Members Suffered Damages

50. The ramifications of T-Mobile's failure to keep PII secure are long lasting and severe. Once PII is stolen, fraudulent use of that information and damage to victims may continue for years. Consumer victims of data breaches are more likely to become victims of identity fraud, occurring 65 percent of the time.[32]

51. In 2019 alone, consumers lost more than $1.9 billion to identity theft and fraud.[33]

52. Besides the monetary damage sustained, consumers may also spend anywhere from approximately 7 hours to upwards to over 1,000 hours trying to resolve identity theft issues.[34]

53. Plaintiff and members of the Class now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. The Class are incurring and will continue to incur such damages in addition to any fraudulent use of their PII.

---

[32] https://www.identityforce.com/blog/identity-theft-odds-identity-theft-statistics#:~:text=In%202019%2C%2014.4%20million%20consumers,about%201%20in%2015%20people&text=Identity%20theft%20is%20the%20most,data%20breaches%20increased%20by%2017%25

[33] *Id.*

[34] https://www.lifelock.com/learn-identity-theft-resources-how-long-does-it-take-to-recover-from-identity-theft.html#:~:text=And%20ID%20theft%20recovery%20is,more%20resolving%20identity%20theft%20problems.

54. Despite all of the publicly available knowledge of the continued compromises of PII, T-Mobile's approach to maintaining the privacy of PII was reckless, or in the very least, negligent.

55. As a result of T-Mobile's failure to prevent the Data Breach, Plaintiff and members of the Class have suffered and will continue to suffer injuries, including loss of time and productivity through efforts to ameliorate, mitigate, and deal with the future consequences of the Data Breach; theft of their valuable PII; the imminent and certainly impeding injury flowing from fraud and identity theft posed by their PII being placed in the hands of criminals; damages to and diminution in value of their PII that was entrusted to Defendant with the understanding the Defendant would safeguard the PII against disclosure; and continued risk to Plaintiff's and the Class Members' PII, which remains in the possession of Defendant and which is subject to further breaches so long as Defendant fail to undertake appropriate and adequate measures to protect the PII that was entrusted to them.

CLASS ALLEGATIONS

56. Plaintiff brings this case individually and, pursuant to Rule 23 of the Federal Rules of Civil Procedure, on behalf of the following class:

> All individuals in the United States whose PII was compromised in the T-Mobile Data Breach which occurred around August 2021.

57. Excluded from the Class is Defendant, its subsidiaries and affiliates, its officers, directors and members of their immediate families and any entity in which Defendant has a controlling interest, the legal representative, heirs, successors, or assigns of any such excluded party, the judicial officer(s) to whom this action is assigned, and the members of their immediate families.

58. Plaintiff reserves the right to modify or amend the definition of the proposed Class if necessary before this Court determines whether certification is appropriate.

59. The requirements of Rule 23(a)(1) are satisfied. The class described above is so numerous that joinder of all individual members in one action would be impracticable. The disposition of the individual claims of the respective class members through this class action will benefit both the parties and this Court. The exact size of the class and the identities of the individual members thereof are ascertainable through Defendant's records, including but not limited to, the files implicated in the Data Breach.

60. The requirements of Rule 23(a)(2) are satisfied. There is a well-defined community of interest and there are common questions of fact and law affecting members of the Class. The questions of fact and law common to the Class predominate over questions which may affect individual members and include the following:

a. Whether and to what extent Defendant had a duty to protect the PII of Plaintiff and Class Members;

b. Whether Defendant was negligent in collecting and storing Plaintiff's and Class Members' PII;

c. Whether Defendant had duties not to disclose the PII of Class Members to unauthorized third parties;

d. Whether Defendant took reasonable steps and measures to safeguard Plaintiff's and Class Members' PII;

e. Whether Defendant failed to adequately safeguard the PII of Plaintiff and Class Members;

f. Whether Defendant breached their duties to exercise reasonable care in handling Plaintiff's and Class Members' PII by storing that information unencrypted on computers and hard drives in the manner alleged herein, including failing to comply with industry standards;

g. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

h. Whether Defendant had respective duties not to use the PII of Plaintiff and Class Members for non-business purposes;

i. Whether Defendant adequately, promptly, and accurately informed Plaintiff and Class Members that their PII had been compromised;

j. Whether Plaintiff and Class Members are entitled to damages as a result of Defendant's wrongful conduct; and

k. Whether Plaintiff and Class Members are entitled to injunctive relief to redress the imminent and currently ongoing harm faced as a result of the Data Breach.

61. The requirements of Rule 23(a)(3) are satisfied. Plaintiff's claims are typical of the claims of the members of the Class. The claims of the Plaintiff and members of the Class are based on the same legal theories and arise from the same failure by Defendant to safeguard PII.

62. Plaintiff and members of the Class were customers of T-Mobile, each having their PII obtained by an unauthorized third party.

63. The requirements of Rule 23(a)(4) are satisfied. Plaintiff is an adequate representative of the Class because his interests do not conflict with the interests of the members of the Class. Plaintiff will fairly, adequately, and vigorously represent and protect the interests of

the members of the Class and have no interests antagonistic to the members of the Class. In addition, Plaintiff has retained counsel who are competent and experienced in the prosecution of class action litigation. The claims of Plaintiff and members of the Class are substantially identical as explained above. While the aggregate damages that may be awarded to the members of the Class are likely to be substantial, the damages suffered by the individual members of the Class are relatively small. As a result, the expense and burden of individual litigation make it economically infeasible and procedurally impracticable for each member of the Class to individually seek redress for the wrongs done to them. Certifying the case as a class will centralize these substantially identical claims in a single proceeding, which is the most manageable litigation method available to Plaintiff and the Class and will conserve the resources of the parties and the court system, while protecting the rights of each member of the Class. Defendant's uniform conduct is generally applicable to the Class as a whole, making relief appropriate with respect to each Class member.

FIRST CAUSE OF ACTION
NEGLIGENCE
(On Behalf of Plaintiff and the Class)

64. Plaintiff restates and realleges all proceeding allegations above as if fully set forth herein.

65. T-Mobile owed a duty under common law to Plaintiff and the Class Members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting and protecting their PII in its possession from being compromised, lost, stolen, accessed and misused by unauthorized persons. More specifically, this duty included, among other things: (a) designing, maintaining, and testing T-Mobile's security systems to ensure that Plaintiff's and Class Members' PII in T-Mobile's possession was adequately secured and protected; (b) implementing processes that would detect a breach of its security system in a timely manner; (c) timely acting upon warning

and alerts, including those generated by its own security systems, regarding intrusions to its networks; and (d) maintaining data security measures consistent with industry standards.

66. T-Mobile's duty to use reasonable care arose from several sources, including but not limited to those described below.

67. T-Mobile had a common law duty to prevent foreseeable harm to others. This duty existed because Plaintiff and Class Members were the foreseeable and probable victims of any inadequate security practices on the part of Defendant. By collecting and storing valuable PII that is routinely targeted by criminals for unauthorized access, T-Mobile was obligated to act with reasonable care to protect against these foreseeable threats.

68. T-Mobile admits that it has the responsibility to protect consumer data, that it is entrusted with this data, and that it did not live up to its responsibility to protect the PII at issue here.

69. T-Mobile breached the duties owed to Plaintiff and Class Members and thus was negligent. T-Mobile breached these duties by, among other things, failing to: (a) exercise reasonable care and implement adequate security systems, protocols and practices sufficient to protect the PII of Plaintiff and Class Members; (b) detect the breach while it was ongoing; (c) maintain security systems consistent with industry standards; and (d) disclose that Plaintiff's and Class Members' PII in T-Mobile's possession had been or was reasonably believed to have been, stolen or compromised.

70. But for T-Mobile's wrongful and negligent breach of its duties owed to Plaintiff and Class Members, their PII would not have been compromised.

71. As a direct and proximate result of T-Mobile's negligence, Plaintiff and Class Members have suffered injuries, including:

a. Theft of their PII;

b. Costs associated with requested credit freezes;

c. Costs associated with the detection and prevention of identity theft;

d. Costs associated with purchasing credit monitoring and identity theft protection services;

e. Lowered credit scores resulting from credit inquiries following fraudulent activities;

f. Costs associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate, mitigate, and deal with the actual and future consequences of the T-Mobile Data Breach;

g. The imminent and certainly impending injury flowing from potential fraud and identity theft posed by their PII being placed in the hands of criminals;

h. Damages to and diminution in value of their PII entrusted, directly or indirectly, to T-Mobile with the mutual understanding that T-Mobile would safeguard Plaintiff's and Class Members data against theft and not allow access and misuse of their data by others; and

i. Continued risk of exposure to hackers and thieves of their PII, which remains in T-Mobile's possession and is subject to further breaches so long as T-Mobile fails to undertake appropriate and adequate measures to protect Plaintiff.

72. As a direct and proximate result of T-Mobile's negligence, Plaintiff and Class Members are entitled to damages, including compensatory, punitive, and/or nominal damages, in an amount to be proven at trial.

SECOND CAUSE OF ACTION
NEGLIGENCE PER SE
(On Behalf of Plaintiff and the Class)

73. Plaintiff restates and realleges all proceeding factual allegations above as if fully set forth herein.

74. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce" including, as interpreted and enforced by the FTC, the unfair act or practice by companies such as T-Mobile for failing to use reasonable measures to protect PII. Various FTC publications and orders also form the basis of T-Mobile's duty.

75. T-Mobile violated Section 5 of the FTC Act by failing to use reasonable measures to protect PII and not complying with the industry standards. T-Mobile's conduct was particularly unreasonable given the nature and amount of PII it obtained and stored and the foreseeable consequences of a data breach.

76. T-Mobile's violation of Section 5 of the FTC Act constitutes negligence *per se*.

77. Plaintiff and Class Members are consumers within the class of persons Section 5 of the FTC Act was intended to protect. Moreover, the harm that has occurred is the type of harm that the FTC Act was intended to guard against. Indeed, the FTC has pursued over fifty enforcement actions against businesses which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm suffered by Plaintiff and Class Members.

78. As a direct and proximate result of T-Mobile's negligence, Plaintiff and Class Members have been injured as described herein and in Paragraph 71 above, and are entitled to damages, including compensatory, punitive, and nominal damages, in an amount to be proven at trial.

THIRD CAUSE OF ACTION
DECLARATORY JUDGMENT
(On Behalf of Plaintiff and the Class)

79. Plaintiff restates and realleges all proceeding allegations above as if fully set forth herein.

80. Under the Declaratory Judgment Act, 28 U.S.C. §§ 2201, *et seq.*, this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and grant further necessary relief. Furthermore, the Court has broad authority to restrain acts, such as here, that are tortious and violate the terms of the federal and state statutes described in this Complaint.

81. An actual controversy has arisen in the wake of the Data Breach regarding Plaintiff's and Class Members' PII and whether T-Mobile is currently maintaining data security measures adequate to protect Plaintiff's and Class Members from further data breaches that compromise their PII. Plaintiff alleges that T-Mobile's data security measures remain inadequate. T-Mobile publicly denies these allegations. Furthermore, Plaintiff continue to suffer injury as a result of the compromise of their PII and remain at imminent risk that further compromises of their PII will occur in the future.

82. Pursuant to its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following:

a. T-Mobile owes a legal duty to secure consumers' PII and to timely notify consumers of a data breach under the common law, and Section 5 of the FTC Act; and

b. T-Mobile continues to breach this legal duty by failing to employ reasonable measures to secure consumers' PII.

83. This Court also should issue corresponding prospective injunctive relief requiring T-Mobile to employ adequate security protocols consistent with law and industry standards to protect consumers' PII.

84. If an injunction is not issued, Plaintiff will suffer irreparable injury, and lack an adequate legal remedy, in the event of another data breach at T-Mobile. The risk of another such breach is real, immediate, and substantial. If another breach at T-Mobile occurs, Plaintiff and Class Members will not have an adequate remedy at law because many of the resulting injuries are not readily quantified and they will be forced to bring multiple lawsuits to rectify the same conduct.

85. The hardship to Plaintiff if an injunction is not issued exceeds the hardship to T-Mobile if an injunction is issued. Plaintiff will likely be subjected to substantial identity theft and other damage. On the other hand, the cost to T-Mobile of complying with an injunction by employing reasonable prospective data security measures is relatively minimal, and T-Mobile has a pre-existing legal obligation to employ such measures.

86. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing another data breach at T-Mobile, thus eliminating the additional injuries that would result to Plaintiff and consumers whose confidential information would be further compromised.

PRAYER FOR RELIEF

WHEREFORE Plaintiff on behalf of himself and all other similarly situated, prays for relief as follows:

a. For an order certifying the Class under Rule 23 of the Federal Rules of Civil Procedure and naming Plaintiff as representative of the Class and Plaintiff's attorneys as Class Counsel to represent the Class;

b. For an order finding in favor of Plaintiff and the Class on all counts asserted herein;

c. For damages in an amount to be determined by the trier of fact;

d. For an order of restitution and all other forms of equitable monetary relief;

e. Declaratory and injunctive relief as described herein;

f. Awarding Plaintiff's reasonable attorneys' fees, costs, and expenses;

g. Awarding pre- and post-judgment interest on any amounts awarded; and,

h. Awarding such other and further relief as may be just and proper.

JURY TRIAL DEMAND

A jury trial is demanded on all claims so triable.

Dated: January 28, 2022

Respectfully submitted,

/s/ David M. Skeens
David M. Skeens – Mo. Bar #35728
WALTERS RENWICK RICHARDS SKEENS & VAUGHAN PC
1100 Main Street, Suite 2500
Kansas City, MO 64105
Telephone: (816) 421-6620
dskeens@wrrsvlaw.com

(Eddie) Jae K. Kim (*pro hac vice* forthcoming)
LYNCH CARPENTER, LLP
117 East Colorado Blvd., Suite 600
Pasadena, CA 91105
Telephone: (626) 550-1250
ekim@lcllp.com

Gary F. Lynch (*pro hac vice* forthcoming)
Nicholas A. Colella (*pro hac vice* forthcoming)
LYNCH CARPENTER, LLP
1133 Penn Avenue, 5th Floor
Pittsburgh, PA 15222
Telephone: (412) 322-9243
Facsimile: (412) 231-0246
gary@lcllp.com
nickc@lcllp.com

Attorneys for Plaintiff