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").

TERRELL MARSHALL LAW GROUP PLLC
936 North 34th Street, Suite 300
Seattle, Washington 98103-8869
TEL. 206.816.6603 • FAX 206.319.5450
www.terrellmarshall.com

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*.

TERRELL MARSHALL LAW GROUP PLLC
936 North 34th Street, Suite 300
Seattle, Washington 98103-8869
TEL. 206.816.6603 • FAX 206.319.5450
www.terrellmarshall.com

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

TERRELL MARSHALL LAW GROUP PLLC
936 North 34th Street, Suite 300
Seattle, Washington 98103-8869
TEL. 206.816.6603 • FAX 206.319.5450
www.terrellmarshall.com

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

TERRELL MARSHALL LAW GROUP PLLC
936 North 34th Street, Suite 300
Seattle, Washington 98103-8869
TEL. 206.816.6603 • FAX 206.319.5450
www.terrellmarshall.com

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).

TERRELL MARSHALL LAW GROUP PLLC
936 North 34th Street, Suite 300
Seattle, Washington 98103-8869
TEL. 206.816.6603 • FAX 206.319.5450
www.terrellmarshall.com

27. In the course of collecting Private Information from customers and potential customers, including Plaintiffs and Class Members, Defendant promises to provide confidentiality and security for customers' and potential customer's Private Information, including by promulgating and placing privacy policies on its website.

28. In the T-Mobile Privacy Notice (hereinafter "Privacy Notice"), which is effective as of May 5, 2021 and provided on Defendant's website, Defendant states that "[Customers] trust T-Mobile to connect [customers] to the world every day, and we're working hard to earn a place in [customers'] heart[s]. A big part of that is maintaining [customer] privacy." [5]

29. Further in the Privacy Notice, Defendant promises to protect consumer's Private Information and that it uses "administrative, technical, contractual, and physical safeguards designed to protect [customer] data while it is under our control." [6]

30. However, Defendant failed to protect and safeguard Plaintiffs' and Class Members' Private Information. In fact, there is no indication that Defendant followed even its most basic promises. For example, T-Mobile does not claim that any of the stolen Private Information was encrypted, including usernames and passwords.

B. The Data Breach

31. On or about August 15, 2021, media reports indicated that T-Mobile was "investigating a forum post claiming to be selling a mountain of personal data" that had come from T-Mobile servers that contained personal customer data. [7]

32. The reports also claimed that a portion of the stolen T-Mobile customer data, including "30 million Social Security numbers and drivers licenses," were being sold on the dark web for approximately $270,000. [8]

---

[5] *T-Mobile Privacy Notice*, T-Mobile, https://www.t-mobile.com/privacy-center/our-practices/privacy-policy (last visited Aug. 19, 2021).
[6] *Id*.
[7] *See* Joseph Cox, *T-Mobile Investigating Claims of Massive Customer Data Breach*, Vice (Aug. 15, 2021), https://www.vice.com/en/article/akg8wg/tmobile-investigating-customer-data-breach-100-million (last visited Aug. 19, 2021).
[8] *Id*.

TERRELL MARSHALL LAW GROUP PLLC
936 North 34th Street, Suite 300
Seattle, Washington 98103-8869
TEL. 206.816.6603 • FAX 206.319.5450
www.terrellmarshall.com

33. On August 16, 2021, T-Mobile released a statement that a sophisticated cyberattack had enabled "unauthorized access to some T-Mobile data" by cyberthieves and that it had launched an investigation into the Data Breach. [9]

34. On August 17, 2021, T-Mobile released a statement saying that "[while] 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."[10]

35. On August 19, 2021, T-Mobile posted a "Notice of Data Breach" on its website, confirming that: "T-Mobile learned that a bad actor illegally accessed personal data. Our investigation is ongoing, but we have verified that a subset of T-Mobile data had been accessed by unauthorized individuals and the data stolen from our systems did include some personal information." [11]

36. Also on August 19, 2019, T-Mobile began texting the following notice, in part, to Class Members, including Plaintiffs Espanoza and Morales: "T-Mobile has determined that unauthorized access to some of your personal data has occurred."

37. In addition, the initial investigation discovered that "7.8 million current T-Mobile postpaid customer accounts' information appears to be contained in the stolen files, as well as just over 40 million records of former or prospective customers who had previously applied for credit with T-Mobile." [12]

38. T-Mobile also confirmed that the cyberthieves accessed and stole "customers' first and last names, date of birth, SSN, and driver's license/ID information for a subset of

[9] *T-Mobile Cybersecurity Incident Update*, T-Mobile (Aug. 16, 2021), https://www.t-mobile.com/news/network/cybersecurity-incident-update-august-2021 (last visited Aug. 19, 2021).
[10] *Supra*, note 1.
[11] *See Notice of Data Breach: Keeping You Safe from Cybersecurity Threats*, T-Mobile (Aug. 19, 2021), https://www.t-mobile.com/brand/data-breach-2021 (last visited Aug. 19, 2021).
[12] *Supra*, note 1.

TERRELL MARSHALL LAW GROUP PLLC
936 North 34th Street, Suite 300
Seattle, Washington 98103-8869
TEL. 206.816.6603 • FAX 206.319.5450
www.terrellmarshall.com

current and former postpay customers and prospective T-Mobile customers[,]" as well as "850,000 active T-Mobile prepaid customer names, phone numbers and account PINs[.]" [13]

39. At this time, Defendant has not indicated how long the unauthorized third-party had unfettered access to sensitive, protected, and confidential customer information stored on Defendant's network, such as Plaintiffs' and Class Members' Private Information. Had Defendant taken its data security obligations more seriously, Defendant would have discovered and stopped the unauthorized intrusion sooner.

40. Upon information and belief, the cyberattack was targeted at Defendant due to its status as a leading telecommunications company that collects and maintains valuable Private Information, such as Social Security numbers and financial information.

41. The targeted cyberattack was expressly designed to gain access to private and confidential data, including (among other things) the Private Information of current, former, and prospective customers, like Plaintiffs and the Class Members.

42. Because of this targeted cyberattack, data thieves were able to gain access to Defendant's servers and subsequently access and exfiltrate the protected Private Information of Plaintiffs and Class Members.

43. By Defendant's own admission, "we have now been able to confirm that the data stolen from our systems did include some personal information" which means that Plaintiffs' and Class Members Private Information was exfiltrated as well, not merely viewed without authorization.

44. The files accessed by this incident contained the following information: names, dates of birth, phone numbers, drivers' licenses, government identification numbers, Social Security numbers, and T-Mobile account PINs

45. There is no indication that the Private Information contained in the stolen files was encrypted.

[13] *Id*.

TERRELL MARSHALL LAW GROUP PLLC
936 North 34th Street, Suite 300
Seattle, Washington 98103-8869
TEL. 206.816.6603 • FAX 206.319.5450
www.terrellmarshall.com

46. Plaintiffs' Private Information was accessed and stolen in the Data Breach. Plaintiffs further believe their stolen Private Information was subsequently sold on the Dark Web.

47. Defendant's offer of twenty-four months of complimentary credit monitoring services is an acknowledgment by T-Mobile that the impacted individuals are subject to a present and ongoing threat of fraud and identity theft.

48. Defendant had obligations created by contract, industry standards, common law, and representations made to Plaintiffs and Class Members to keep their Private Information confidential and to protect it from unauthorized access and disclosure.

49. Plaintiffs and Class Members provided their Private Information to Defendant with the reasonable expectation, and mutual understanding, that Defendant would comply with its obligations to keep such information confidential and secure from unauthorized access.

C. Defendant Was Aware of the Risks of a Data Breach

50. Defendant had obligations created by contract, industry standards, common law, and representations made to Plaintiffs and Members of the Classes, to keep their Private Information confidential and to protect it from unauthorized access and disclosure.

51. Plaintiffs and Class Members provided their Private Information to Defendant with the reasonable expectation and mutual understanding that Defendant would comply with its obligations to keep such information confidential and secure from unauthorized access.

52. Defendant's data security obligations were particularly important given the substantial increase in cyber-attacks and/or data breaches preceding the date of the breach.

53. Data breaches have become widespread. For example, the United States saw 1,244 data breaches in 2018 and had 446.5 million exposed records. [14]

[14] *98 Must-Know Data Breach Statistics for 2021*, Varonis, https://blogvaronis2.wpengine.com/data-breach-statistics/ (last visited Aug. 19, 2021).

TERRELL MARSHALL LAW GROUP PLLC
936 North 34th Street, Suite 300
Seattle, Washington 98103-8869
TEL. 206.816.6603 • FAX 206.319.5450
www.terrellmarshall.com

54. Defendant clearly understood this reality because a quote, posted on Defendant's website, by a senior manager of T-Mobiles Cyber Architecture & Controls unit stated that:

> At T-Mobile, everyone is challenge[d] to think outside of conventional approaches to digital security; all know assumptions are reevaluated. We work on forward-thinking technologies, including micro-segmentation, machine learning, predictive analytics, web situational awareness, advance threat mitigation, active defense, data obfuscation and next-generation endpoint technologies it. [15]

55. However, T-Mobile failed to take fully implement data security systems and protect critical Private Information belonging to consumers.

56. Indeed, data breaches, such as the one experienced by Defendant, have become so notorious that the Federal Bureau of Investigation ("FBI") and U.S. Secret Service have issued a warning to potential targets, so they are aware of, and prepared for, a potential attack. Therefore, the increase in such attacks, and attendant risk of future attacks, was widely known and completely foreseeable to the public and to anyone in Defendant's industry, including Defendant.

57. According to the Federal Trade Commission ("FTC"), identity theft wreaks havoc on consumers' finances, credit history, and reputation and can take time, money, and patience to resolve.[16] Identity thieves use stolen personal information for a variety of crimes, including government benefits fraud, phone or utilities fraud, and bank and finance fraud. [17]

---

[15] *Digital Security*, T-Mobile, https://www.t-mobile.com/careers/digital-security (last visited Aug. 19, 2021).
[16] *See Taking Charge, What to Do If Your Identity is Stolen*, FTC, 3 (Apr. 2013), https://dss.mo.gov/cd/older-youth-program/files/taking-charge-what-to-do-if-identity-is-stolen.pdf (last visited Aug. 19, 2021).
[17] *Id*. The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority." 16 CFR § 603.2. The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, social security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number." *See Taking Charge, What to Do If Your Identity is Stolen, FTC, 3 (Apr. 2013),* https://dss.mo.gov/cd/older-youth-program/files/taking-charge-what-to-do-if-identity-is-stolen.pdf (last visited Aug. 19, 2021).

TERRELL MARSHALL LAW GROUP PLLC
936 North 34th Street, Suite 300
Seattle, Washington 98103-8869
TEL. 206.816.6603 • FAX 206.319.5450
www.terrellmarshall.com

58. The Private Information of Plaintiffs and Members of the Classes was taken by hackers to engage in identity theft or and or to sell it to other criminals who will purchase the Private Information for that purpose. The fraudulent activity resulting from the Data Breach may not come to light for years.

59. Defendant knew, or reasonably should have known, of the importance of safeguarding the Private Information of Plaintiffs and Members of the Classes, including Social Security numbers, driver's license, and/or dates of birth, and of the foreseeable consequences that would occur if Defendant's data security systems were breached, including, specifically, the significant costs that would be imposed on Plaintiffs and Members of the Classes a result of a breach.

60. Plaintiffs and Members of the Classes now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. The Classes are incurring and will continue to incur such damages in addition to any fraudulent use of their Private Information.

61. The injuries to Plaintiffs and Members of the Classes were directly and proximately caused by Defendant's failure to implement or maintain adequate data security measures for the Private Information of Plaintiffs and Members of the Classes.

D. Defendant Failed to Comply with FTC Guidelines

62. The FTC has promulgated numerous guides for businesses which 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.

63. In 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which established cyber-security guidelines for businesses. The guidelines note that businesses should protect the personal customer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to

TERRELL MARSHALL LAW GROUP PLLC
936 North 34th Street, Suite 300
Seattle, Washington 98103-8869
TEL. 206.816.6603 • FAX 206.319.5450
www.terrellmarshall.com

correct any security problems. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.

64. The FTC further recommends that companies not maintain Private Information longer than is needed for authorization of a transaction; limit access to sensitive 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.

65. The FTC has brought enforcement actions against businesses for failing to protect consumer data adequately and reasonably, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

66. Defendant failed to properly implement basic data security practices, and their failure to employ reasonable and appropriate measures to protect against unauthorized access to consumer Private Information constitutes an unfair act or practice prohibited by Section 5 of the FTCA, 15 U.S.C. § 45.

67. Defendant was at all times fully aware of their obligation to protect the Private Information of current, former, and prospective customers. Defendant was also aware of the significant repercussions that would result from their failure to do so.

E. Defendant Failed to Comply with Industry Standards

68. A number of industry and national best practices have been published and should have been used as a go-to resource and authoritative guide when developing Defendant's cybersecurity practices.

TERRELL MARSHALL LAW GROUP PLLC
936 North 34th Street, Suite 300
Seattle, Washington 98103-8869
TEL. 206.816.6603 • FAX 206.319.5450
www.terrellmarshall.com

69. Best cybersecurity practices that are standard in Defendant's industry include encrypting files; installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches and routers; monitoring and protection of physical security systems; protection against any possible communication system; and training staff regarding critical points.

70. Defendant failed to meet the minimum standards of the following cybersecurity frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are established standards in reasonable cybersecurity readiness.

71. These foregoing frameworks are existing and applicable industry standards in Defendant's industry, and Defendant failed to comply with these accepted standards, thereby opening the door to the Cyber-Attack and causing the Data Breach.

F. Defendant's Breach

72. T-Mobile breached its obligations to Plaintiffs and Class Members and/or was otherwise negligent and reckless because it failed to properly maintain and safeguard its computer systems and data. T-Mobile's unlawful conduct includes, but is not limited to, the following acts and/or omissions:

a. Failing to maintain an adequate data security system to reduce the risk of data breaches and cyberattacks;

b. Failing to adequately protect current, former, and prospective customers' Private Information;

c. Failing to properly monitor its own data security systems for existing intrusions;

TERRELL MARSHALL LAW GROUP PLLC
936 North 34th Street, Suite 300
Seattle, Washington 98103-8869
TEL. 206.816.6603 • FAX 206.319.5450
www.terrellmarshall.com

d. Failing to comply with FTC guidelines for cybersecurity, in violation of Section 5 of the FTC Act, and;

e. Failing to adhere to industry standards for cybersecurity.

73. T-Mobile negligently and unlawfully failed to safeguard Plaintiffs' and Class Members' Private Information.

74. Accordingly, as outlined below, Plaintiffs and Class Members now face an increased risk of fraud and identity theft. In addition, Plaintiffs and the Class Members also lost the benefit of the bargain they made with T-Mobile.

G. The Value of Private Information to Cyber Criminals and Increased Risk of Fraud and Identity Theft to Consumers

75. Businesses that store personal information are likely to be targeted by cyber criminals. Credit card and bank account numbers are tempting targets for hackers. However, information such as dates of birth and Social Security numbers are even more attractive to hackers; they are not easily destroyed and can be easily used to perpetrate identity theft and other types of fraud.

76. The Private Information of individuals remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials. For example, personal information can be sold at a price ranging from $40 to $200, and bank details have a price range of $50 to $200. [18]

77. Social Security numbers, for example, are among the worst kind of personal information to have stolen because they may be put to a variety of fraudulent uses and are difficult for an individual to change. The Social Security Administration ("SSA") stresses that the loss of an individual's Social Security number, as is the case here, can lead to identity theft and extensive financial fraud:

[18] *See Your personal data is for sale on the dark web. Here's how much it costs,* Digital Trends, (Oct. 16, 2019), https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs (last visited Aug. 19, 2021).

TERRELL MARSHALL LAW GROUP PLLC
936 North 34th Street, Suite 300
Seattle, Washington 98103-8869
TEL. 206.816.6603 • FAX 206.319.5450
www.terrellmarshall.com

> A dishonest person who has your Social Security number can use it to get other personal information about you. Identity thieves can use your number and your good credit to apply for more credit in your name. Then, they use the credit cards and don't pay the bills, it damages your credit. You may not find out that someone is using your number until you're turned down for credit, or you begin to get calls from unknown creditors demanding payment for items you never bought. Someone illegally using your Social Security number and assuming your identity can cause a lot of problems.[19]

78. What is more, it is no easy task to change or cancel a stolen Social Security number. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. In other words, preventive action to defend against the possibility of misuse of a Social Security number is not permitted; an individual must show evidence of actual, ongoing fraud activity to obtain a new number.

79. Even then, a new Social Security number may not be effective. According to Julie Ferguson of the Identity Theft Resource Center, "The credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number." [20]

80. Furthermore, as the SSA warns:

> Keep in mind that a new number probably will not solve all your problems. This is because other governmental agencies (such as the IRS and state motor vehicle agencies) and private businesses (such as banks and credit reporting companies) likely will have records under your old number. Along with other personal information, credit reporting companies use the number to identify your credit record. So using a new number will not guarantee you a fresh start. This is especially true if your other personal information, such as your name and address, remains the same.
> If you receive a new Social Security Number, you should not be able to use the old number anymore.

---

[19] *Identity Theft and Your Social Security Number*, Social Security Administration (2018); *available at*: https://www.ssa.gov/pubs/EN-05-10064.pdf (last visited Aug. 19, 2021).

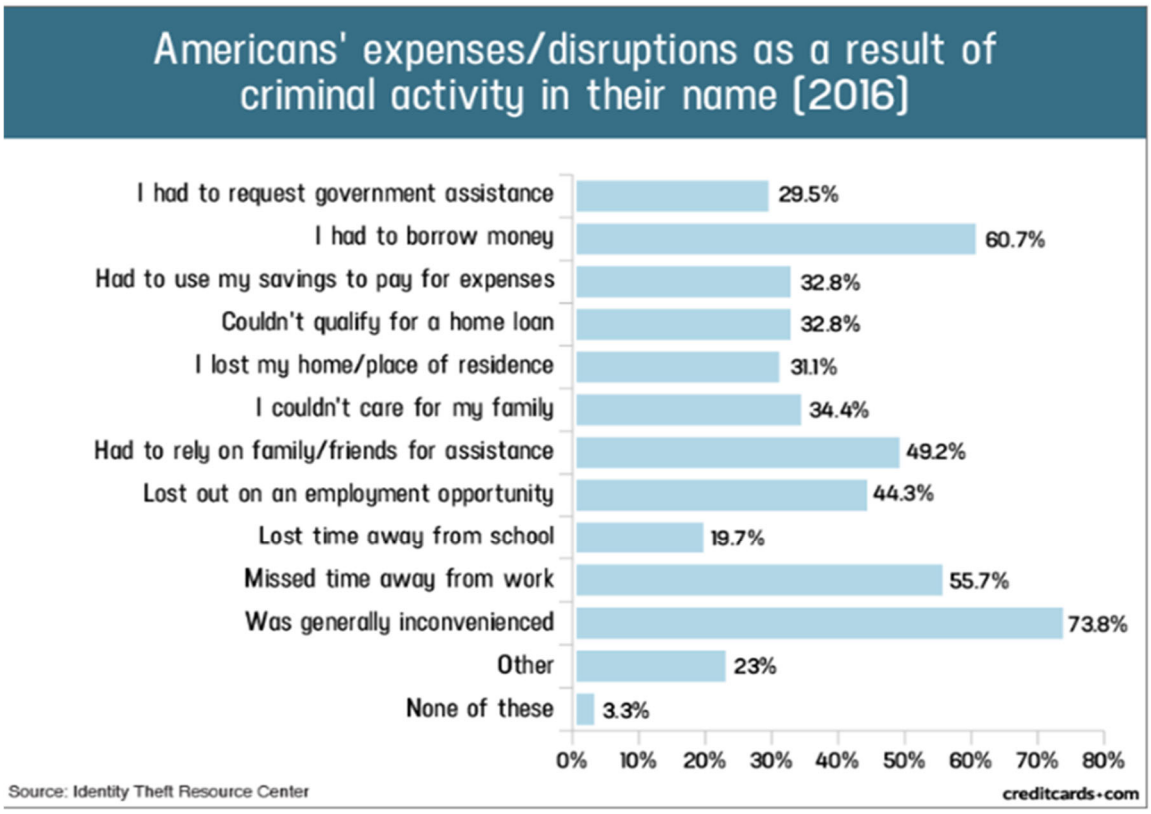
[20] Bryan Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR (Feb. 9, 2015), http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millionsworrying-about-identity-theft (last visited Aug. 19, 2021).

TERRELL MARSHALL LAW GROUP PLLC
936 North 34th Street, Suite 300
Seattle, Washington 98103-8869
TEL. 206.816.6603 • FAX 206.319.5450
www.terrellmarshall.com

> For some victims of identity theft, a new number actually creates new problems. If the old credit information is not associated with your new number, the absence of any credit history under the new number may make more difficult for you to get credit. [21]

81. Here, the unauthorized access left the cyber criminals with the tools to perform the most thorough identity theft—they have obtained all the essential Private Information to mimic the identity of the user. The personal data of Plaintiffs and Members of the Classes stolen in the Data Breach constitutes a dream for hackers and a nightmare for Plaintiffs and the Classes.

82. A study by Identity Theft Resource Center shows the multitude of harms caused by fraudulent use of personal and financial information: [22]



[21] *Supra*, note 18.

[22] *See* Jason Steele, *Credit Card and ID Theft Statistics*, CreditCards.com (Oct. 23, 2020) https://www.creditcards.com/credit-card-news/credit-card-security-id-theft-fraud-statistics-1276.php (last visited Aug. 19, 2021).

TERRELL MARSHALL LAW GROUP PLLC
936 North 34th Street, Suite 300
Seattle, Washington 98103-8869
TEL. 206.816.6603 • FAX 206.319.5450
www.terrellmarshall.com

83. Stolen personal data of Plaintiffs and Members of the Classes represents essentially one-stop shopping for identity thieves.

84. The FTC has released its updated publication on protecting Private Information for businesses, which includes instructions on protecting Private Information, properly disposing of Private Information, understanding network vulnerabilities, implementing policies to correct security problems, using intrusion detection programs, monitoring data traffic, and having in place a response plan.

85. General policy reasons support such an approach. A person whose personal information has been compromised may not see any signs of identity theft for years. According to the United States Government Accountability Office ("GAO") Report to Congressional Requesters:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm. [23]

86. Companies recognize that Private Information is a valuable asset. Indeed, Private Information is a valuable commodity. A "cyber black-market" exists in which criminals openly post stolen Social Security numbers and other Private Information on a number of Internet websites. The stolen personal data of Plaintiff and members of the Classes has a high value on both legitimate and black markets.

87. Identity thieves may commit various types of crimes such as immigration fraud, obtaining a driver's license or identification card in the victim's name but with another's

[23] *See* U.S. Gov. Accounting Office, GAO-07-737, *Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown* (2007) at 29, *available at:* https://www.gao.gov/new.items/d07737.pdf (last visited Aug. 19, 2021).

TERRELL MARSHALL LAW GROUP PLLC
936 North 34th Street, Suite 300
Seattle, Washington 98103-8869
TEL. 206.816.6603 • FAX 206.319.5450
www.terrellmarshall.com

picture, and/or using the victim's information to obtain a fraudulent tax refund or fraudulent unemployment or COVID-19 relief benefits. The United States government and privacy experts acknowledge that it may take years for identity theft to come to light and be detected.

88. As noted above, the disclosure of Social Security numbers in particular poses a significant risk. Criminals can, for example, use Social Security numbers to create false bank accounts or file fraudulent tax returns. Defendant's current, former, and prospective customers whose Social Security numbers have been compromised now face a present and imminent risk of identity theft and other problems associated with the disclosure of their Social Security number and will need to monitor their credit and tax filings for an indefinite duration.

89. Based on the foregoing, the information compromised in the Data Breach is significantly more valuable than the loss of, for example, credit card information in a retailer data breach, because, there, victims can cancel or close credit and debit card accounts. The information compromised in this Data Breach is impossible to "close" and difficult, if not impossible, to change — Social Security number, driver's license number or government-issued identification number, name, and date of birth.

90. This data demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "Compared to credit card information, personally identifiable information and Social Security numbers are worth more than 10x on the black market." [24]

91. Among other forms of fraud, identity thieves may obtain driver's licenses, government benefits, medical services, and housing or even give false information to police.

92. According to a recent article in the New York Times, cyber thieves are using illegally obtained driver's to submit and fraudulently obtain unemployment benefits.[25] An

[24] Tim Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, IT World, (Feb. 6, 2015), https://www.networkworld.com/article/2880366/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html (last visited Aug. 19, 2021).

[25] *How Identity Thieves Took My Wife for a Ride*, New York Times, (April 27, 2021) https://www.nytimes.com/2021/04/27/your-money/identity-theft-auto-insurance.html (last visited Aug. 19, 2021)

TERRELL MARSHALL LAW GROUP PLLC
936 North 34th Street, Suite 300
Seattle, Washington 98103-8869
TEL. 206.816.6603 • FAX 206.319.5450
www.terrellmarshall.com

individual may not know that his or her driver's license was used to file for unemployment benefits until law enforcement notifies the individual's employer of the suspected fraud, or until the individual attempts to lawfully apply for unemployment and is denied benefits (due to the prior, fraudulent application and award of benefits).

H. The Plaintiffs' Experiences

1. Plaintiff Stephanie M. Espanoza

93. Plaintiff Stephanie Espanoza opened her cellular telephone postpaid customer account with Defendant in or about June 2006 and was required to provide, among other things, her full name, date of birth and Social Security number.

94. On or about August 16, 2021, Plaintiff Espanoza, and the public, was first notified of the Data Breach by T-Mobile and that cybercriminals had illegally accessed and stole confidential customer data from millions of T-Mobile customer accounts. In addition, Plaintiff Espanoza received the August 19, 2021 text message from T-Mobile notifying her that her Private Information was among the confidential data that cybercriminals illegally accessed and stole from Defendant's servers.

95. As a direct and proximate result of the breach, Plaintiff Espanoza has made reasonable efforts to mitigate the impact of the breach, including but not limited to: purchasing credit protection, researching the internet concerning this Data Breach; discussing the breach with her family; reviewing credit reports and financial account statements for any indications of actual or attempted identity theft or fraud; and researching credit monitoring and identity theft protection services offered by Defendant. This is valuable time Plaintiff Espinoza otherwise could have and would have spent on other activities, including but not limited to taking care of her 10-month old daughter, work and/or recreation.

96. Plaintiff Espinoza is very concerned about identity theft, her banking account and fraud, as well as the consequences of such identity theft and fraud resulting from the Data Breach.

TERRELL MARSHALL LAW GROUP PLLC
936 North 34th Street, Suite 300
Seattle, Washington 98103-8869
TEL. 206.816.6603 • FAX 206.319.5450
www.terrellmarshall.com

97. Plaintiff Espinoza suffered actual injury from having Private Information compromised as a result of the Data Breach including, but not limited to (a) damage to and diminution in the value of his Private Information, a form of property that Defendant obtained from Plaintiff; (b) violation of Plaintiffs' privacy rights; and (c) present and increased risk arising from the identity theft and fraud.

98. Plaintiff Espinoza has and will spend a significant amount of time responding to the impacts of the Data Breach. The time spent dealing with the fallout from the Data Breach is time Plaintiff otherwise would have spent on other activities, such as caring for her newborn, work and/or recreation.

99. As a result of the Data Breach, Plaintiff Espinoza anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. As a result of the Data Breach, Plaintiff is and will continue to be at increased risk of identity theft and fraud for years to come.

2. <u>Plaintiff Jonathan Morales</u>

100. Plaintiff Jonathan Morales is a T-Mobile cellular customer and was required to provide to Defendant, among other things, his full name and Social Security number.

101. On or about August 17, 2021, Plaintiff Morales, and the public, was first notified of the Data Breach by T-Mobile and that cybercriminals had illegally accessed and stole confidential customer data from millions of T-Mobile customer accounts. In addition, Plaintiff Morales received the August 19, 2021 text message from T-Mobile notifying him that his Private Information was among the confidential data that cybercriminals illegally accessed and stole from Defendant's servers.

102. As a direct and proximate result of the breach, Plaintiff Morales has made reasonable efforts to mitigate the impact of the breach, including but not limited to: researching the Data Breach; reviewing credit reports and financial account statements for any indications of actual or attempted identity theft or fraud; and researching credit monitoring and

TERRELL MARSHALL LAW GROUP PLLC
936 North 34th Street, Suite 300
Seattle, Washington 98103-8869
TEL. 206.816.6603 • FAX 206.319.5450
www.terrellmarshall.com

identity theft protection services offered by Defendant. This is valuable time Plaintiff Morales otherwise would have spent on other activities, including but not limited to work and/or recreation.

103. Plaintiff Morales is very concerned about identity theft and fraud, as well as the consequences of such identity theft and fraud resulting from the Data Breach.

104. Plaintiff Morales suffered actual injury from having Private Information compromised as a result of the Data Breach including, but not limited to (a) damage to and diminution in the value of his Private Information, a form of property that Defendant obtained from Plaintiff; (b) violation of Plaintiffs' privacy rights; and (c) present and increased risk arising from the identity theft and fraud.

105. Moreover, subsequent to the Data Breach, Plaintiff Morales also experienced a significant increase in the amount of suspicious, unsolicited phishing spam. Plaintiff Morales receives a substantial amount of spam, all of which appear to be placed with the intent to obtain personal information to commit identity theft by way of a social engineering attack.

106. Plaintiff Morales has and will spend a significant amount of time responding to the impacts of the Data Breach. The time spent dealing with the fallout from the Data Breach is time Plaintiff otherwise would have spent on other activities, such as work and/or recreation.

107. As a result of the Data Breach, Plaintiff Morales anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. As a result of the Data Breach, Plaintiff is and will continue to be at increased risk of identity theft and fraud for years to come.

3. Plaintiff Alex Pygin

108. Plaintiff Alex Pygin opened his cellular telephone postpaid customer account with Defendant in or about August 2019 and was required to provide, among other things, his full name and Social Security number.

TERRELL MARSHALL LAW GROUP PLLC
936 North 34th Street, Suite 300
Seattle, Washington 98103-8869
TEL. 206.816.6603 • FAX 206.319.5450
www.terrellmarshall.com

109. On or about August 17, 2021, Plaintiff Pygin, and the public, was first notified of the Data Breach by T-Mobile and that cybercriminals had illegally accessed and stole confidential customer data from millions of T-Mobile customer accounts. [26]

110. As a direct and proximate result of the breach, Plaintiff Pygin has made reasonable efforts to mitigate the impact of the breach, including but not limited to: researching the Data Breach; reviewing credit reports and financial account statements for any indications of actual or attempted identity theft or fraud; and researching credit monitoring and identity theft protection services offered by Defendant. This is valuable time Plaintiff Pygin otherwise would have spent on other activities, including but not limited to work and/or recreation.

111. Plaintiff Pygin is very concerned about identity theft and fraud, as well as the consequences of such identity theft and fraud resulting from the Data Breach.

112. Plaintiff Pygin suffered actual injury from having Private Information compromised as a result of the Data Breach including, but not limited to (a) damage to and diminution in the value of his Private Information, a form of property that Defendant obtained from Plaintiff; (b) violation of Plaintiffs' privacy rights; and (c) present and increased risk arising from the identity theft and fraud.

113. Plaintiff Pygin has and will spend a significant amount of time responding to the impacts of the Data Breach. The time spent dealing with the fallout from the Data Breach is time Plaintiff otherwise would have spent on other activities, such as work and/or recreation.

114. As a result of the Data Breach, Plaintiff Pygin anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. As a result of the Data Breach, Plaintiff is and will continue to be at increased risk of identity theft and fraud for years to come.

[26] *Supra*, note 1.

TERRELL MARSHALL LAW GROUP PLLC
936 North 34th Street, Suite 300
Seattle, Washington 98103-8869
TEL. 206.816.6603 • FAX 206.319.5450
www.terrellmarshall.com

I. Plaintiffs' and Class Members' Damages

115. To date, Defendant has done absolutely nothing to provide Plaintiffs and Class Members with relief for the damages they have suffered because of the Data Breach, including, but not limited to, the costs and loss of time they incurred because of the Data Breach.

116. Defendant has only offered inadequate identity monitoring services. Defendant places the burden squarely on Plaintiffs and Class Members by requiring them to expend time signing up for that service, as opposed to automatically enrolling all victims of this cybercrime. In addition, Defendant only offers these services for two years, even though experts agree that the effects of such a data breach can often be felt by victims for around seven years.

117. Plaintiffs' and Class Members' Private Information were compromised as a direct and proximate result of the Data Breach.

118. As a direct and proximate result of Defendant's conduct, Plaintiffs and Class Members are in imminent, immediate, and continuing increased risk of harm from fraud and identity theft.

119. As a direct and proximate result of Defendant's conduct, Plaintiffs and Class Members have been forced to expend time dealing with the effects of the Data Breach.

120. Plaintiffs and Class Members face a present and substantial risk of out-of-pocket fraud losses such as loans opened in their names, government benefits fraud, tax return fraud, utility bills opened in their names, credit card fraud, and similar identity theft.

121. Plaintiffs and Class Members face a present and substantial risk of being targeted for future phishing, data intrusion, and other illegal schemes based on their Private Information as potential fraudsters could use that information to target such schemes more effectively to Plaintiffs and Class Members.

122. Plaintiffs and Class Members have and may continue to incur out-of-pocket costs for protective measures such as credit monitoring fees, credit report fees, credit freeze fees, and similar costs directly or indirectly related to the Data Breach.

TERRELL MARSHALL LAW GROUP PLLC
936 North 34th Street, Suite 300
Seattle, Washington 98103-8869
TEL. 206.816.6603 • FAX 206.319.5450
www.terrellmarshall.com

123. Plaintiffs and Class Members also suffered a loss of value of their Private Information when it was acquired by cyber thieves in the Data Breach. Numerous courts have recognized the propriety of loss of value damages in related cases.

124. Plaintiffs and Class Members have spent and will continue to spend significant amounts of time to monitor their financial accounts for misuse. Indeed, Defendant's own Notice of Data Breach page posted on its website states that the stolen data is in "harm's way" and encourages Plaintiffs and Class Members to "take proactive steps regularly to protect your data and identity[.]" [27]

125. Plaintiffs and Class Members have suffered or will suffer actual injury as a direct result of the Data Breach. Many victims suffered ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach relating to:

a. Finding fraudulent charges, loans, and/or government benefit claims;

b. Purchasing credit monitoring and identity theft prevention;

c. Placing "freezes" and "alerts" with credit reporting agencies;

d. Spending time on the phone with or at a financial institution or government agency to dispute fraudulent charges and/or claims;

e. Contacting financial institutions and closing or modifying financial accounts;

f. Closely reviewing and monitoring Social Security numbers, bank accounts, and credit reports for unauthorized activity for years to come.

126. Moreover, Plaintiffs and Class Members have an interest in ensuring that their Private Information, which is believed to remain in the possession of Defendant, is protected from further breaches by the implementation of security measures and safeguards, including but not limited to, making sure that the storage of data or documents containing personal and

[27] *Notice of Data Breach: Keeping You Safe from Cybersecurity Threats*, T-Mobile (Aug. 19, 2021), https://www.t-mobile.com/brand/data-breach-2021 (last visited Aug. 19, 2021).

TERRELL MARSHALL LAW GROUP PLLC
936 North 34th Street, Suite 300
Seattle, Washington 98103-8869
TEL. 206.816.6603 • FAX 206.319.5450
www.terrellmarshall.com

financial information is not accessible online, that access to such data is password-protected, and that such data is properly encrypted.

127. As a direct and proximate result of Defendant's actions and inactions, Plaintiffs and Class Members have suffered a loss of privacy and are at an imminent and increased risk of future harm.

128. To date, Defendant has done absolutely nothing to provide Plaintiffs and Class members with relief for the damages they have suffered because of the Data Breach, including, but not limited to, the costs and loss of time they incurred because of the Data Breach.

129. Defendant has only offered inadequate identity monitoring services, and it is unclear whether that credit monitoring was only offered to certain affected individuals (based upon the type of data stolen), or to all persons whose data was compromised in the Data Breach. What is more, Defendant places the burden squarely on Plaintiffs and Class members by requiring them to expend time signing up for that service, as opposed to automatically enrolling all victims of this cybercrime.

V. CLASS ALLEGATIONS

130. Plaintiffs bring this nationwide class action pursuant to rules 23(b)(2), 23(b)(3), and 23(c)(4) of the Federal Rules of Civil Procedure, individually and on behalf of all members of the following class:

> All current, former, and prospective T-Mobile customers residing in the United States whose Private Information was compromised in the Data Breach announced by Defendant on or about August 16, 2021 (the "Nationwide Class").

131. The California Subclass is defined as follows:

> All current, former, and prospective T-Mobile customers residing in California whose Private Information was compromised in the Data Breach announced by Defendant on or about August 16, 2021 (the "California Subclass").

TERRELL MARSHALL LAW GROUP PLLC
936 North 34th Street, Suite 300
Seattle, Washington 98103-8869
TEL. 206.816.6603 • FAX 206.319.5450
www.terrellmarshall.com

132. The California Subclass is referred to herein as the "Statewide Subclass" and together with the Nationwide Class, are collectively referred to herein as the "Classes."

133. Excluded from the Classes are all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out, and all judges assigned to hear any aspect of this litigation and their immediate family members.

134. Plaintiffs reserve the right to modify or amend the definitions of the proposed Classes before the Court determines whether certification is appropriate.

135. **Numerosity:** The Classes are so numerous that joinder of all members is impracticable. Defendant has identified millions of current, former, and prospective customers whose Private Information may have been improperly accessed in the Data Breach, and the Classes are apparently identifiable within Defendant's records.

136. **Commonality:** Questions of law and fact common to the Classes exist and predominate over any questions affecting only individual members of the Classes. These include:

a. When Defendant actually learned of the Data Breach and whether their response was adequate;

b. Whether Defendant owed a duty to the Classes to exercise due care in collecting, storing, safeguarding and/or obtaining their Private Information;

c. Whether Defendant breached that duty;

d. Whether Defendant implemented and maintained reasonable security procedures and practices appropriate to the nature of storing the Private Information of Plaintiffs and Members of the Classes;

e. Whether Defendant acted negligently in connection with the monitoring and/or protection of Private Information belonging to Plaintiffs and Members of the Classes;

TERRELL MARSHALL LAW GROUP PLLC
936 North 34th Street, Suite 300
Seattle, Washington 98103-8869
TEL. 206.816.6603 • FAX 206.319.5450
www.terrellmarshall.com

f. Whether Defendant knew or should have known that it did not employ reasonable measures to keep the Private Information of Plaintiffs and Members of the Classes secure and to prevent loss or misuse of that Private Information;

g. Whether Defendant adequately addressed and fixed the vulnerabilities which permitted the Data Breach to occur;

h. Whether Defendant caused Plaintiffs' and Members of the Classes damage;

i. Whether Defendant violated the law by failing to promptly notify Plaintiffs and Members of the Classes that their Private Information had been compromised;

j. Whether Defendant violated the consumer protection statutes invoked below; and

k. Whether Plaintiffs and the other Members of the Classes are entitled to credit monitoring and other monetary relief;

137. **Typicality:** Plaintiffs' claims are typical of those of the other Members of the Classes because all had their Private Information compromised as a result of the Data Breach due to Defendant's misfeasance.

138. **Adequacy:** Plaintiffs will fairly and adequately represent and protect the interests of the members of the Classes. Plaintiffs' Counsel are competent and experienced in litigating privacy-related class actions.

139. **Superiority and Manageability:** Under rule 23(b)(3) of the Federal Rules of Civil Procedure, a class action is superior to other available methods for the fair and efficient adjudication of this controversy since joinder of all the members of the Classes is impracticable. Individual damages for any individual member of the Classes are likely to be insufficient to justify the cost of individual litigation, so that in the absence of class treatment, Defendant's misconduct would go unpunished. Furthermore, the adjudication of this controversy through a

TERRELL MARSHALL LAW GROUP PLLC
936 North 34th Street, Suite 300
Seattle, Washington 98103-8869
TEL. 206.816.6603 • FAX 206.319.5450
www.terrellmarshall.com

class action will avoid the possibility of inconsistent and potentially conflicting adjudication of the asserted claims. There will be no difficulty in the management of this action as a class action.

140. Class certification is also appropriate under Rule 23(a) and (b)(2) because Defendant acted or refused to act on grounds generally applicable to the Classes, so that final injunctive relief or corresponding declaratory relief is appropriate as to the Nationwide Class as a whole and as to the Subclass as a whole.

141. Likewise, particular issues under Rule 23(c)(4) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

a. Whether Defendant owed a legal duty to Plaintiffs and Members of the Classes to exercise due care in collecting, storing, using, and safeguarding their Private Information;

b. Whether Defendant breached a legal duty to Plaintiffs and the Members of the Classes to exercise due care in collecting, storing, using, and safeguarding their Private Information;

c. Whether Defendant failed to comply with its own policies and applicable laws, regulations, and industry standards relating to data security;

d. 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; and

e. Whether members of the Classes are entitled to actual damages, credit monitoring or other injunctive relief, and/or punitive damages as a result of Defendant's wrongful conduct.

TERRELL MARSHALL LAW GROUP PLLC
936 North 34th Street, Suite 300
Seattle, Washington 98103-8869
TEL. 206.816.6603 • FAX 206.319.5450
www.terrellmarshall.com

VI. FIRST CLAIM FOR RELIEF

Negligence (On Behalf of Plaintiffs, the Nationwide Class, and the Statewide Subclass)

142. Plaintiffs re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 141.

143. Defendant owed a common law duty to Plaintiffs and Members of the Classes to exercise reasonable care in obtaining, using, and protecting their Private Information from unauthorized third parties.

144. The legal duties owed by Defendant to Plaintiffs and Members of the Classes include, but are not limited to the following:

a. To exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the Private Information of Plaintiffs and Members of the Classes in its possession;

b. To protect Private Information of Plaintiffs and Members of the Classes in its possession using reasonable and adequate security procedures that are compliant with industry-standard practices; and

c. To implement processes to quickly detect a data breach and to timely act on warnings about data breaches, including promptly notifying Plaintiffs and Members of the Classes of the Data Breach.

145. Defendant's duty to use reasonable data security measures also arose under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45(a) (the "FTC Act"), which prohibits "unfair . . . practices in or affecting commerce," including, as interested and enforced by the Federal Trade Commission, the unfair practices by companies such as Defendant of failing to use reasonable measures to protect Private Information.

146. Various FTC publications and data security breach orders further form the basis of Defendant's duty. Plaintiffs and Members of the Classes are consumers under the FTC Act. Defendant violated Section 5 of the FTC Act by failing to use reasonable measures to protect Private Information and by not complying with industry standards.

TERRELL MARSHALL LAW GROUP PLLC
936 North 34th Street, Suite 300
Seattle, Washington 98103-8869
TEL. 206.816.6603 • FAX 206.319.5450
www.terrellmarshall.com

147. Defendant breached its duties to Plaintiffs and Members of the Classes. Defendant knew or should have known the risks of collecting and storing Private Information and the importance of maintaining secure systems, especially in light of the fact that data breaches have been surging in the past 5 years.

148. Defendant knew or should have known that its security practices did not adequately safeguard the Private Information belonging to the Plaintiffs and Members of the Classes.

149. Through Defendant's acts and omissions described in this Complaint, including Defendant's failure to provide adequate security and its failure to protect the Private Information of Plaintiffs and Members of the Classes from being foreseeably captured, accessed, exfiltrated, stolen, disclosed, and misused, Defendant unlawfully breached its duty to use reasonable care to adequately protect and secure the Private Information of Plaintiffs and Members of the Classes during the period it was within Defendant's possession and control.

150. Defendant breached the duties it owed to Plaintiffs and Members of the Classes in several ways, including:

a. Failing to implement adequate security systems, protocols, and practices sufficient to protect current, former, and prospective customers' Private Information, including Plaintiffs and Members of the Classes, and thereby creating a foreseeable risk of harm;

b. Failing to comply with the minimum industry data security standards prior to the Data Breach;

c. Failing to act despite knowing or having reason to know that its systems were vulnerable to attack; and

151. Due to Defendant's conduct, Plaintiffs and Members of the Classes are entitled to credit monitoring. Credit monitoring is reasonable here. The Private Information taken can be used for identity theft and other types of financial fraud against Plaintiffs and Members of the Classes.

TERRELL MARSHALL LAW GROUP PLLC
936 North 34th Street, Suite 300
Seattle, Washington 98103-8869
TEL. 206.816.6603 • FAX 206.319.5450
www.terrellmarshall.com

152. Some experts recommend that data breach victims obtain credit monitoring services for at least ten years following a data breach. Annual subscriptions for credit monitoring plans range from approximately $219 to $358 per year. [28]

153. As a result of Defendant's negligence, Plaintiffs and Members of the Classes suffered injuries that may include: (i) the lost or diminished value of Private Information; (ii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their Private Information; (iii) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, including, but not limited to, time spent deleting phishing scams and reviewing and monitoring sensitive accounts; (iv) the present and continued risk to their Private Information, which may remain for sale on the dark web and is in Defendant's possession and subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information in their continued possession; (v) future costs in terms of time, effort, and money that will be expended to prevent, monitor, detect, contest, and repair the impact of the Data Breach for the remainder of the lives of Plaintiffs and Members of the Classes, including ongoing credit monitoring.

154. These injuries were reasonably foreseeable given the history of security breaches of this nature. The injury and harm that Plaintiff and the members of the Classes suffered was the direct and proximate result of Defendant's negligent conduct.

VII. SECOND CLAIM FOR RELIEF

Negligence *Per Se* (On Behalf of Plaintiffs, the Nationwide Class, and the Statewide Subclass)

155. Plaintiffs re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 141.

[28] In the recent Equifax data breach, for example, Equifax agreed to free monitoring of victims' credit reports at all three major credit bureaus for four years, plus $1 million of identity theft insurance. For an additional six years, victims can opt for free monitoring by one credit bureau, Equifax. In addition, if a victim's child was a minor in May 2017, he or she is eligible for a total of 18 years of free credit monitoring under the same terms as for adults.

TERRELL MARSHALL LAW GROUP PLLC
936 North 34th Street, Suite 300
Seattle, Washington 98103-8869
TEL. 206.816.6603 • FAX 206.319.5450
www.terrellmarshall.com

156. 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 businesses, such as Defendant's, of failing to use reasonable measures to protect Private Information. The FTC publications and orders described above also form part of the basis of Defendant's duty in this regard.

157. Defendant violated Section 5 of the FTC Act by failing to use reasonable measures to protect Private Information and not complying with applicable industry standards. Defendant's conduct was particularly unreasonable given the nature and amount of Private Information it obtained and stored, and the foreseeable consequences of the Data Breach for companies of Defendant's magnitude, including, specifically, the immense damages that would result to Plaintiffs and Members of the Classes due to the valuable nature of the Private Information at issue in this case—including Social Security numbers.

158. Defendant's violations of Section 5 of the FTC Act constitute negligence per se.

159. Plaintiffs and Members of the Classes are within the class of persons that the FTC Act was intended to protect.

160. The harm that occurred as a result of the Data Breach is the type of harm the FTC Act was intended to guard against. The FTC has pursued enforcement actions against businesses, which, as a result of its failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiffs and Members of the Classes.

161. As a direct and proximate result of Defendant's negligence per se, Plaintiffs and Members Classes have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity how their Private Information is used; (iii) the compromise, publication, and/or theft of their Private Information; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their Private Information; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and

TERRELL MARSHALL LAW GROUP PLLC
936 North 34th Street, Suite 300
Seattle, Washington 98103-8869
TEL. 206.816.6603 • FAX 206.319.5450
www.terrellmarshall.com

future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from tax fraud and identity theft; (vi) costs associated with placing freezes on credit reports; (vii) the present and continued risk to their Private Information, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information of its current, former, and prospective customers in its continued possession; and (viii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the Private Information compromised as a result of the Data Breach for the remainder of the lives of Plaintiffs and Members of the Classes.

162. Additionally, as a direct and proximate result of Defendant's negligence *per se*, Plaintiffs and Members of the Classes have suffered and will suffer the continued risks of exposure of their Private Information, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information in their continued possession.

VIII. THIRD CLAIM FOR RELIEF

Breach of Implied Contract

(On Behalf of Plaintiffs, the Nationwide Class, and the Statewide Subclass)

163. Plaintiffs re-allege and incorporate by reference Paragraphs 1 through 141 above as if fully set forth herein.

164. Defendant provided Plaintiffs and Class Members with an implied contract to protect and keep confidential Defendant's current, former, and prospective customers' private, nonpublic personal and financial information when they gathered the information from each of their current, former, and prospective customers.

165. Plaintiffs and Class Members would not have provided their personal and financial information to Defendant, but for Defendant's implied promises to safeguard and

TERRELL MARSHALL LAW GROUP PLLC
936 North 34th Street, Suite 300
Seattle, Washington 98103-8869
TEL. 206.816.6603 • FAX 206.319.5450
www.terrellmarshall.com

protect Defendant's current, former, and prospective customers private personal and financial information.

166. Plaintiffs and Class Members performed their obligations under the implied contract when they provided their private personal and financial information in exchange for telecommunication services provided by Defendant.

167. Defendant breached the implied contracts with Plaintiffs and Class Members by failing to protect and keep private the nonpublic personal and financial information provided to them about Plaintiffs and Class Members.

168. As a direct and proximate result of Defendant's breach of their implied contracts, Plaintiffs and Class Members have been harmed and have suffered, and will continue to suffer, damages and injuries.

IX. FOURTH CLAIM FOR RELIEF

Violations of California's Consumer Legal Remedies Act Cal. Civ. Code § 1750, *et seq.*

(On Behalf of Plaintiffs and the Statewide Subclass)

169. Plaintiffs re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 141.

170. Plaintiffs bring this claim individually and on behalf of the Members of the Statewide Subclass.

171. Defendant's conduct constitutes violations under California's Legal Remedies Act, Cal. Civ. Code § 1750, *et seq*. (the "CLRA").

172. Defendant's conduct falls within the meaning of this statute because they caused transactions resulting in the sale or lease of goods or services to consumers – namely, the sale of cellular products and services to consumers. Such as Plaintiffs and Class Members. The sale of these cellular services is considered services within the meaning of the statute under Civil Code § 1761(b).

TERRELL MARSHALL LAW GROUP PLLC
936 North 34th Street, Suite 300
Seattle, Washington 98103-8869
TEL. 206.816.6603 • FAX 206.319.5450
www.terrellmarshall.com

173. Plaintiffs and Members of the Statewide Subclass are consumers pursuant to this statute.

174. Defendant violated the Consumer Legal Remedies Act by way of Civil Code § 1770(a)(5). In particular, Defendant represented (and continues to represent) that their services have benefits and characteristics which they do not have – mainly that Defendant has adequate data security practices to ensure that consumers' Private Information is safe and secure from unauthorized disclosure.

175. Defendant is aware that this misrepresentation, which is a significant factor for its commercial success, is false and misleading.

176. Plaintiffs and Members of the Statewide Class seek injunctive or other equitable relief to ensure that Defendant hereinafter adequately safeguards Private Information by implementing reasonable security procedures and practices. This relief is important because Defendant still holds Private Information related to Plaintiffs and Members of the Statewide Class. Plaintiffs and Members of the California Class have an interest in ensuring that their Private Information is reasonably protected.

177. Pursuant to Cal. Civ. Code § 1782, on August 20, 2011, Plaintiffs will mail Defendant notice in writing, via U.S. certified mail, of the particular violations of Cal. Civ. Code § 1770 of the CLRA and demand that they rectify the actions described above by providing complete monetary relief, agreeing to be bound by Defendant's legal obligations and to give notice to all affected customers of their intent to do so. If Defendant fails to take the actions demanded to rectify their violations of the CLRA, Plaintiffs will seek statutory damages and attorneys' fees as allowed by the CLRA.

X. FIFTH CLAIM FOR RELIEF

Violation of the Washington State Consumer Protection Act (RCW 19.86.010 *et seq*.)

(On Behalf of Plaintiffs and the Nationwide Class)

TERRELL MARSHALL LAW GROUP PLLC
936 North 34th Street, Suite 300
Seattle, Washington 98103-8869
TEL. 206.816.6603 • FAX 206.319.5450
www.terrellmarshall.com

178. Plaintiffs re-allege and incorporate by reference Paragraphs 1 through 141 above as if fully set forth herein.

179. The Washington State Consumer Protection Act, RCW 19.86.020 (the "CPA") prohibits any "unfair or deceptive acts or practices" in the conduct of any trade or commerce as those terms are described by the CPA and relevant case law.

180. Defendant is a "person" as described in RWC 19.86.010(1).

181. Defendant engages in "trade" and "commerce" as described in RWC 19.86.010(2) in that they engage in selling telecommunication products and services, that directly and indirectly affect the people of the State of Washington.

182. By virtue of the above-described wrongful actions, inaction, omissions, and want of ordinary care that directly and proximately caused the Data Breach, Defendant engaged in unlawful, unfair and fraudulent practices within the meaning, and in violation of, the CPA, in that Defendant's practices were injurious to the public interest because they injured other persons, had the capacity to injure other persons, and have the capacity to injure other persons.

183. In the course of conducting their business, Defendant committed "unfair or deceptive acts or practices" by*, inter alia,* knowingly failing to design, adopt, implement, control, direct, oversee, manage, monitor and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems to safeguard and protect Plaintiffs and Class Members' Private Information, and violating the common law alleged herein in the process. Plaintiffs and Class Members reserve the right to allege other violations of law by Defendant constituting other unlawful business acts or practices. Defendant's above-described wrongful actions, inaction, omissions, and want of ordinary care are ongoing and continue to this date.

184. The gravity of Defendant's wrongful conduct outweighs any alleged benefits attributable to such conduct. There were reasonably available alternatives to further

TERRELL MARSHALL LAW GROUP PLLC
936 North 34th Street, Suite 300
Seattle, Washington 98103-8869
TEL. 206.816.6603 • FAX 206.319.5450
www.terrellmarshall.com

Defendant's legitimate business interests other than engaging in the above-described wrongful conduct.

185. As a direct and proximate result of Defendant's above-described wrongful actions, inaction, omissions, and want of ordinary care that directly and proximately caused the Data Breach and its violations of the CPA, Plaintiffs and Class Members have suffered, and will continue to suffer, economic damages and other injury and actual harm in the form of, *inter alia*, (1) an imminent, immediate and the continuing increased risk of identity theft, identity fraud and medical fraud—risks justifying expenditures for protective and remedial services for which they are entitled to compensation; (2) invasion of privacy; (3) breach of the confidentiality their Private Information; (5) deprivation of the value of their Private Information, for which there is a well-established national and international market; and/or (v) the financial and temporal cost of monitoring credit, monitoring financial accounts, and mitigating damages.

186. Unless restrained and enjoined, Defendant will continue to engage in the above-described wrongful conduct and more data breaches will occur. Plaintiffs, therefore, on behalf of themselves, Class Members, and the general public, also seeks restitution and an injunction prohibiting Defendant from continuing such wrongful conduct, and requiring Defendant to modify their corporate culture and design, adopt, implement, control, direct, oversee, manage, monitor and audit appropriate data security processes, controls, policies, procedures protocols, and software and hardware systems to safeguard and protect the Private Information entrusted to it.

187. Plaintiffs, on behalf of themselves and the Class Members also seek to recover actual damages sustained by each class member together with the costs of the suit, including reasonable attorney fees. In addition, the Plaintiffs, on behalf of themselves and the Class Members request that this Court use its discretion, pursuant to RCW 19.86.090, to increase the damages award for each Class Member by three times the actual damages sustained not to exceed $25,000.00 per class member.

TERRELL MARSHALL LAW GROUP PLLC
936 North 34th Street, Suite 300
Seattle, Washington 98103-8869
TEL. 206.816.6603 • FAX 206.319.5450
www.terrellmarshall.com

XI. SIXTH CLAIM FOR RELIEF

Unjust Enrichment (On Behalf of Plaintiffs, the Nationwide Class, and the Statewide Subclass)

188. Plaintiffs re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 141.

189. Defendant benefited from receiving Plaintiffs' and Members of the Classes' Private Information by its ability to retain and use that information for its own benefit. Defendant understood this benefit.

190. Defendant also understood and appreciated that Plaintiffs' and Members of the Classes' Private Information was private and confidential, and its value depended upon Defendant maintaining the privacy and confidentiality of that Private Information.

191. Plaintiffs' and Members of the Classes who were customers of Defendant's customer conferred a monetary benefit upon Defendant in the form of monies paid for services available from Defendant.

192. Defendant appreciated or had knowledge of the benefits conferred upon them by Plaintiff and members of the Classes. Defendant also benefited from the receipt of Plaintiffs' and Members of the Classes' Private Information, as Defendant used it to facilitate the transfer of Private Information between parties.

193. The monies that Plaintiffs' and Members of the Classes paid to Defendant for services were to be used by Defendant, in part, to pay for the administrative costs of reasonable data privacy and security practices and procedures.

194. Defendant also understood and appreciated that Plaintiffs' and Members of the Classes' Private Information was private and confidential, and its value depended upon Defendant maintaining the privacy and confidentiality of that Private Information.

195. But for Defendant's willingness and commitment to maintain privacy and confidentiality, that Private Information would not have been transferred to and entrusted with Defendant. Indeed, if Defendant had informed Plaintiffs' and Members of the Classes that their

TERRELL MARSHALL LAW GROUP PLLC
936 North 34th Street, Suite 300
Seattle, Washington 98103-8869
TEL. 206.816.6603 • FAX 206.319.5450
www.terrellmarshall.com

data and cyber security measures were inadequate, Defendant would not have been permitted to continue to operate in that fashion by regulators, its shareholders, and its consumers.

196. As a result of Defendant's wrongful conduct, Defendant was unjustly enriched at the expense of, and to the detriment of, Plaintiffs' and Members of the Classes. Defendant continues to benefit and profit from their retention and use of the Private Information while its value to Plaintiffs' and Members of the Classes has been diminished.

197. Defendant's unjust enrichment is traceable to, and resulted directly and proximately from, the conduct alleged in this Complaint, including compiling, using, and retaining Plaintiffs' and Members of the Classes' Private Information, while at the same time failing to maintain that information secured from intrusion and theft by hackers and identity thieves.

198. As a result of Defendant's conduct, Plaintiffs' and Members of the Classes suffered actual damages in an amount equal to the difference in value between the amount Plaintiffs' and Members of the Classes paid for their purchases with reasonable data privacy and security practices and procedures and the purchases they actually received with unreasonable data privacy and security practices and procedures.

199. Under principals of equity and good conscience, Defendant should not be permitted to retain the money belonging to Plaintiffs' and Members of the Classes because Defendant failed to implement (or adequately implement) the data privacy and security practices and procedures that Plaintiffs' and Members of the Classes paid for and that were otherwise mandated by federal, state, and local laws and industry standards.

200. Defendant should be compelled to disgorge into a common fund for the benefit of Plaintiffs' and Members of the Classes all unlawful or inequitable proceeds they received as a result of the conduct alleged herein.

TERRELL MARSHALL LAW GROUP PLLC
936 North 34th Street, Suite 300
Seattle, Washington 98103-8869
TEL. 206.816.6603 • FAX 206.319.5450
www.terrellmarshall.com

XII. SEVENTH CLAIM FOR RELIEF

Violation of the California Consumer Privacy Act,

("CCPA") Cal. Civ. Code §§ 1798.100, *et seq*. (§ 1798.150(a))

(On Behalf of Plaintiffs and the Statewide Subclass)

201. Plaintiffs re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 141.

202. Defendant had a duty to implement and maintain reasonable security procedures and practices with regard to Plaintiffs and Statewide Subclass Members' PII.

203. Plaintiffs and the Statewide Subclass Members provided to Defendant their nonencrypted and nonredacted personal information as defined in §1798.81.5 in the form of their PII.

204. Defendant violated the California Consumer Privacy Act, or CCPA, by failing to prevent Plaintiffs and Statewide Subclass Members' PII from unauthorized access and exfiltration, theft, or disclosure as a result of Defendant's violations of its duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the PII of Plaintiffs and Statewide Class Members.

205. As a direct and proximate result of Defendant's acts, including but not limited to its failure to encrypt its systems and otherwise implement and maintain reasonable security procedures and practices, Plaintiffs' and the Statewide Subclass Members' PII was subjected to unauthorized access and exfiltration, theft, or disclosure as a result of Defendant's violation of the duty.

206. As a direct and proximate result of Defendant's acts, including but not limited to its failure to encrypt its systems and otherwise implement and maintain reasonable security procedures and practices, Plaintiffs and the Statewide Subclass Members were injured and lost money or property, including but not limited the loss of Plaintiffs' and Statewide Class Members' legally protected interest in the confidentiality and privacy of their PII, nominal damages, statutory damages, and additional losses as described above.

TERRELL MARSHALL LAW GROUP PLLC
936 North 34th Street, Suite 300
Seattle, Washington 98103-8869
TEL. 206.816.6603 • FAX 206.319.5450
www.terrellmarshall.com

207. Defendant knew or should have known that its computer systems and data security practices were inadequate to safeguard Plaintiffs' and Statewide Subclass Members' PII and that the risk of a data breach or theft was highly likely. Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the PII of Plaintiff and the Statewide Class Members.

208. Defendant is a corporation organized for the profit or financial benefit of its owners, with annual gross revenues exceeding $25 million, and collects PII as defined in Cal. Civ. Code § 1798.140.

209. Plaintiffs and the Statewide Subclass Members seek injunctive or other equitable relief to ensure Defendant hereinafter adequately safeguards Plaintiffs and the Statewide Subclass Members' PII by implementing reasonable security procedures and practices. Such relief is particularly important because Defendant continues to hold Plaintiffs and the Statewide Subclass Members' PII. These individuals have an interest in ensuring that their PII is reasonably protected.

210. Plaintiffs' counsel will send a notice letter to Defendant's registered service agents via certified mail on August 20, 2021. Assuming Defendant does not cure the Data Breach within 30 days, and Plaintiffs believe any such cure is not possible under these facts and circumstances, Plaintiffs intend to promptly amend this Complaint to seek actual damages and statutory damages of no less than $100 and up to $750 per customer record subject to the Data Breach on behalf of the California Class as authorized by the CCPA.

XIII. EIGHTH CLAIM FOR RELIEF

Violation of the California Unfair Competition Law, Cal. Bus. & Prof. Code § 17200, *et seq*. – Unlawful Business Practices (On Behalf of Plaintiffs and the Statewide Subclass)

211. Plaintiffs and the Statewide Subclass restate and reallege the foregoing Paragraphs 1 through 141 as if fully set forth herein.

TERRELL MARSHALL LAW GROUP PLLC
936 North 34th Street, Suite 300
Seattle, Washington 98103-8869
TEL. 206.816.6603 • FAX 206.319.5450
www.terrellmarshall.com

212. Defendant has violated Cal. Bus. and Prof. Code § 17200, *et seq.,* by engaging in unlawful, unfair or fraudulent business acts and practices and unfair, deceptive, untrue or misleading advertising that constitute acts of "unfair competition" as defined in Cal. Bus. Prof. Code § 17200 with respect to the services provided to the California Class.

213. Defendant engaged in unlawful acts and practices with respect to the services by establishing the sub-standard security practices and procedures described herein; by soliciting and collecting Plaintiffs' and Statewide Subclass Members' PII with knowledge that the information would not be adequately protected; and by storing Plaintiffs' and Statewide Subclass Members' PII in an unsecure environment in violation of California's data breach statute, Cal. Civ. Code § 1798.81.5, which requires Defendant to take reasonable methods of safeguarding the PII of Plaintiffs and the Statewide Subclass Members.

214. In addition, Defendant engaged in unlawful acts and practices by failing to disclose the Data Breach to California Subclass Members in a timely and accurate manner, contrary to the duties imposed by Cal. Civ. Code § 1798.82.

215. As a direct and proximate result of Defendant's unlawful practices and acts, Plaintiffs and the Statewide Subclass Members were injured and lost money or property, including but not limited to the price received by Defendant for the services, the loss of Statewide Subclass Members' legally protected interest in the confidentiality and privacy of their PII, nominal damages, and additional losses as described above.

216. Defendant knew or should have known that Defendant's computer systems and data security practices were inadequate to safeguard Statewide Subclass Members' PII and that the risk of a data breach or theft was highly likely, especially given Defendant's inability to adhere to basic encryption standards and data disposal methodologies. Defendant's actions in engaging in the above-named unlawful practices and acts were negligent, knowing and willful, and/or wanton and reckless with respect to the rights of members of the Statewide Subclass.

217. Statewide Subclass Members seek relief under Cal. Bus. & Prof. Code § 17200, *et seq.,* including, but not limited to, restitution to Plaintiffs and Statewide Subclass Members of

TERRELL MARSHALL LAW GROUP PLLC
936 North 34th Street, Suite 300
Seattle, Washington 98103-8869
TEL. 206.816.6603 • FAX 206.319.5450
www.terrellmarshall.com

money or property that Defendant may have acquired by means of Defendant's unlawful, and unfair business practices, restitutionary disgorgement of all profits accruing to Defendant because of Defendant's unlawful and unfair business practices, declaratory relief, attorneys' fees and costs (pursuant to Cal. Code Civ. Proc. § 1021.5), and injunctive or other equitable relief.

XIV. NINTH CAUSE OF ACTION

Violation of California's Unfair Competition Law, Cal. Bus. & Prof. Code § 17200, *et seq.* – Unfair Business Practices (On Behalf of Plaintiffs and the Statewide Subclass)

218. Plaintiffs and the Statewide Subclass restate and reallege the foregoing Paragraphs 1 through 141 as if fully set forth herein.

219. Defendant engaged in unfair acts and practices with respect to the services by establishing the sub-standard security practices and procedures described herein; by soliciting and collecting Plaintiffs' and Statewide Subclass Members' PII with knowledge that the information would not be adequately protected; by storing Plaintiffs' and Statewide Subclass Members' PII in an unsecure electronic environment; and by failing to properly dispose of equipment containing sensitive PII. These unfair acts and practices were immoral, unethical, oppressive, unscrupulous, unconscionable, and/or substantially injurious to Plaintiffs and Statewide Subclass Members. They were likely to deceive the public into believing their PII was securely stored, when it was not. The harm these practices caused to Plaintiffs and the Statewide Subclass Members outweighed their utility, if any.

220. Defendant engaged in unfair acts and practices with respect to the provision of services by failing to take proper action following the Data Breach to enact adequate privacy and security measures and protect Statewide Subclass Members' PII from further unauthorized disclosure, release, data breaches, and theft. These unfair acts and practices were immoral, unethical, oppressive, unscrupulous, unconscionable, and/or substantially injurious to Plaintiffs and Statewide Subclass Members. They were likely to deceive the public into believing their PII

TERRELL MARSHALL LAW GROUP PLLC
936 North 34th Street, Suite 300
Seattle, Washington 98103-8869
TEL. 206.816.6603 • FAX 206.319.5450
www.terrellmarshall.com

was securely stored, when it was not. The harm these practices caused to Plaintiffs and the Statewide Subclass Members outweighed their utility, if any.

221. As a direct and proximate result of Defendant's acts of unfair practices, Plaintiffs and the Statewide Subclass Members were injured and lost money or property, including but not limited to the price received by Defendant for the services, the loss of Statewide Subclass Members' legally protected interest in the confidentiality and privacy of their PII, nominal damages, and additional losses as described above.

222. Defendant knew or should have known that Defendant's computer systems and data security practices were inadequate to safeguard Statewide Subclass Members' PII and that the risk of a data breach or theft was highly likely, including Defendant failure to properly encrypt and dispose of equipment containing sensitive PII. Defendant's actions in engaging in the above-named unlawful practices and acts were negligent, knowing and willful, and/or wanton and reckless with respect to the rights of members of the Statewide Subclass.

223. Statewide Subclass Members seek relief under Cal. Bus. & Prof. Code § 17200, *et seq*., including, but not limited to, restitution to Plaintiffs and Statewide Subclass Members of money or property that Defendant may have acquired by means of Defendant's unfair business practices, restitutionary disgorgement of all profits accruing to Defendant because of Defendant's unfair business practices, declaratory relief, attorneys' fees and costs (pursuant to Cal. Code Civ. Proc. § 1021.5), and injunctive or other equitable relief.

XV. PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, on behalf of themselves and all Class Members, requests judgment against the Defendant and that the Court grant the following:

A. For an Order certifying the Nationwide Classes or, in the alternative, the Subclass as defined herein, and appointing Plaintiffs and their Counsel to represent the certified Classes;

B. For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiffs' and the Class

TERRELL MARSHALL LAW GROUP PLLC
936 North 34th Street, Suite 300
Seattle, Washington 98103-8869
TEL. 206.816.6603 • FAX 206.319.5450
www.terrellmarshall.com

Members' PII, and from refusing to issue prompt, complete, any accurate disclosures to the Plaintiffs and Class members;

C. For injunctive relief requested by Plaintiffs, including but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Plaintiffs and Class Members, including but not limited to an order:

1. prohibiting Defendant from engaging in the wrongful and unlawful acts described herein;
2. requiring Defendant to protect, including through encryption, all data collected through the course of its business in accordance with all applicable regulations, industry standards, and federal, state or local laws;
3. requiring Defendant to delete, destroy, and purge the personal identifying information of Plaintiffs and Class Members unless Defendant can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiffs and Class Members ;
4. requiring Defendant to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of the personal identifying information of Plaintiffs and Class Members' personal identifying information;
5. prohibiting Defendant from maintaining Plaintiffs' and Class Members' personal identifying information on a cloud-based database;
6. requiring Defendant to engage independent third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis, and ordering

TERRELL MARSHALL LAW GROUP PLLC
936 North 34th Street, Suite 300
Seattle, Washington 98103-8869
TEL. 206.816.6603 • FAX 206.319.5450
www.terrellmarshall.com

Defendant to promptly correct any problems or issues detected by such third-party security auditors;

7. requiring Defendant to engage independent third-party security auditors and internal personnel to run automated security monitoring;

8. requiring Defendant to audit, test, and train its security personnel regarding any new or modified procedures;

9. requiring Defendant to segment data by, among other things, creating firewalls and access controls so that if one area of Defendant's network is compromised, hackers cannot gain access to other portions of Defendant's systems;

10. requiring Defendant to conduct regular database scanning and securing checks;

11. requiring Defendant to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon the employees' respective responsibilities with handling personal identifying information, as well as protecting the personal identifying information of Plaintiffs and class members;

12. requiring Defendant to conduct internal training and education routinely and continually, and on an annual basis to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;

13. requiring Defendant to implement a system of tests to assess its respective employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees' compliance with Defendant's policies, programs, and systems for protecting personal identifying information;

TERRELL MARSHALL LAW GROUP PLLC
936 North 34th Street, Suite 300
Seattle, Washington 98103-8869
TEL. 206.816.6603 • FAX 206.319.5450
www.terrellmarshall.com

14. requiring Defendant to implement, maintain, regularly review, and revise as necessary a threat management program designed to appropriately monitor Defendant's information networks for threats, both internal and external, and assess whether monitoring tools are appropriately configured, tested, and updated;

15. requiring Defendant to meaningfully educate all class members about the threats that they face as a result of the loss of their confidential personal identifying information to third parties, as well as the steps affected individuals must take to protect themselves;

16. requiring Defendant to implement logging and monitoring programs sufficient to track traffic to and from Defendant's servers; and

17. for a period of 10 years, appointing a qualified and independent third party assessor to conduct a SOC 2 Type 2 attestation on an annual basis to evaluate Defendant's compliance with the terms of the Court's final judgment, to provide such report to the Court and to counsel for the class, and to report any deficiencies with compliance of the Court's final judgment; and

D. For an award of damages, including actual, nominal, and consequential damages, as allowed by law in an amount to be determined;

E. For an award of punitive damages;

F. For an award of attorneys' fees, costs, and litigation expenses, as allowed by law;

G. For prejudgment interest on all amounts awarded; and

H. Such other and further relief as this Court may deem just and proper.

XVI. DEMAND FOR JURY TRIAL

Plaintiffs hereby demand that this matter be tried before a jury.

TERRELL MARSHALL LAW GROUP PLLC
936 North 34th Street, Suite 300
Seattle, Washington 98103-8869
TEL. 206.816.6603 • FAX 206.319.5450
www.terrellmarshall.com

RESPECTFULLY SUBMITTED AND DATED this 19th day of August, 2021.

TERRELL MARSHALL LAW GROUP PLLC

By: /s/ Beth E. Terrell, WSBA #26759

Beth E. Terrell, WSBA #26759
Email: bterrell@terrellmarshall.com
936 N. 34th Street, Suite 300
Seattle, Washington 98103
Telephone: (206) 206-816-6603
Facsimile: (206) 319-5450

M. Anderson Berry*
Email: aberry@justice4you.com
CLAYEO C. ARNOLD, A PROFESSIONAL LAW CORP.
865 Howe Avenue
Sacramento, California 95825
Telephone: (916) 777-7777
Facsimile: (916) 924-1829

Gary E. Mason*
Email: gmason@masonllp.com
David K. Lietz*
Email: dlietz@masonllp.com
MASON LIETZ & KLINGER LLP
5101 Wisconsin Avenue NW, Suite 305
Washington, DC 20016
Telephone: (202) 429-2290
Facsimile: (202) 429-2294

Gary M. Klinger*
Email: gklinger@masonllp.com
MASON LIETZ & KLINGER LLP
227 W. Monroe Street, Suite 2100
Chicago, Illinois 60606
Telephone: (202) 429-2290
Facsimile: (202) 429-2294

William Howard*
Email: Billy@TheConsumerProtectionFirm.com
THE CONSUMER PROTECTION FIRM
401 East Jackson Street, Suite 2340
Truist Place
Tampa, Florida 33602
Telephone: (813) 500-1500
Facsimile: (813) 435-2369

Attorneys for Plaintiffs and the Classes

**Pro hac vice forthcoming*

TERRELL MARSHALL LAW GROUP PLLC
936 North 34th Street, Suite 300
Seattle, Washington 98103-8869
TEL. 206.816.6603 • FAX 206.319.5450
www.terrellmarshall.com