

1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28

UNITED STATES DISTRICT COURT  
WESTERN DISTRICT OF WASHINGTON

ANIA VILLALON, individually and on  
behalf of all others similarly situated,

Plaintiff,

v.

T-MOBILE USA, INC.,

Defendant.

Case No. \_\_\_\_\_

**CLASS ACTION COMPLAINT**

**JURY TRIAL DEMANDED**

Plaintiff Ania Villalon (“Plaintiff”), individually and as a class representative for others similarly situated, bring this action against Defendant T-Mobile USA, Inc. (“T-Mobile” or “Defendant”). Plaintiff alleges upon personal knowledge as to her own actions and upon information and belief as to all other matters and believe that reasonable discovery will provide additionally evidentiary for the allegations herein.

**I. NATURE OF THE ACTION**

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

2. As a result of the Data Breach, Plaintiff and approximately 40 million former or prospective customers who applied for credit with T-Mobile, approximately 13 million current

1 postpaid customers, and 850,000 active prepaid customers (the “Class Members”)<sup>1</sup> suffered  
2 present injury and damages in the form of identity theft, out-of-pocket expenses and the value of  
3 the time reasonably incurred to remedy or mitigate the effects of the unauthorized access,  
4 exfiltration, and subsequent criminal misuse of their sensitive and highly personal information.

5 3. The Private Information compromised in the Data Breach includes names, phone  
6 numbers, drivers’ licenses, government identification numbers, Social Security numbers, dates of  
7 birth, and T-Mobile account PINs.<sup>2</sup>

8 4. Plaintiff brings this class action lawsuit on behalf of those similarly situated to  
9 address Defendant’s inadequate safeguarding of Class Members’ Private Information that it  
10 collected and maintained.

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

14 6. The mechanism of the cyberattack and potential for improper disclosure of  
15 Plaintiff’s and Class Members’ Private Information was a known risk to Defendant, and thus  
16 Defendant was on notice that failing to take steps necessary to secure the Private Information  
17 from the risk of a ransomware attack.

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

21 8. Plaintiff’s and Class Members’ Private Information was compromised due to  
22 Defendant’s negligent and/or careless acts and omissions and its failure to adequately protect the  
23 Private Information of its current, former, and prospective clients.

24  
25  
26 <sup>1</sup> 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. 24, 2021).

27 <sup>2</sup> *Id.*

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

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

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

12 12. Plaintiff seeks to remedy these harms on behalf of herself and all similarly  
 13 situated individuals whose Private Information was accessed during the Data Breach.

14 13. Accordingly, Plaintiff brings this action on behalf of all persons whose Private  
 15 Information was compromised as a result of Defendant’s negligence and failure to: (i) adequately  
 16 protect its customer’s Private Information, (ii) warn its current, former, and potential customers  
 17 of their inadequate information security practices, and (iii) effectively monitor their data systems  
 18 for security vulnerabilities and incidents. Defendant’s conduct amounts to negligence and  
 19 violates federal and state statutes.

20 14. Plaintiff seeks remedies including, but not limited to, compensatory damages,  
 21 reimbursement of out-of-pocket costs, and injunctive relief including improvements to  
 22 Defendant’s data security systems, future annual audits, and adequate credit monitoring services  
 23 funded by Defendant.

24 **II. JURISDICTION AND VENUE**

25 15. This Court has subject matter jurisdiction over this action under 28 U.S.C. §  
 26 1332(d) because this is a class action wherein the amount in controversy exceeds the sum or  
 27 value of \$5,000,000, exclusive of interest and costs, there are more than 100 members in the  
 28

1 proposed class, and at least one member of the class is a citizen of a state different from  
2 Defendant.

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

5 17. Venue is proper in this Court pursuant to 28 U.S.C. § 1391 because a substantial  
6 part of the events or omissions giving rise to these claims occurred in, were directed to and/or  
7 emanated from this District. Defendant resides within this judicial district and a substantial part  
8 of the events giving rise to the claims alleged herein occurred within this judicial district.

9 **III. PARTIES**

10 18. Plaintiff Ania Villalon is a citizen of New York, residing in Bronx County, New  
11 York and has been a T-Mobile customer for approximately four (4) years.

12 19. On or about August 16, 2021, Plaintiff Villalon, and the public, was first notified  
13 of the Data Breach by T-Mobile and that cybercriminals had illegally accessed and stole  
14 confidential customer data from millions of T-Mobile customer accounts. On August 19, 2021,  
15 Ms. Villalon received a text message from T-Mobile notifying her that her PII was accessed  
16 without her authorization, exfiltrated, and/or stolen in the Data Breach.

17 20. As a direct and proximate result of the breach, Plaintiff Villalon has made  
18 reasonable efforts to mitigate the impact of the breach, including but not limited to: checking  
19 bank accounts for any indication of actual or attempted identity theft or fraud, researching the  
20 internet concerning this Data Breach; discussing the breach with her friends and family; and  
21 reviewing credit reports for any indications of actual or attempted identity theft or fraud. This is  
22 valuable time Plaintiff Villalon otherwise could have and would have spent on other activities,  
23 including but not limited to work and/or recreation.

24 21. On August 22, 2021, shortly after T-Mobile announced the Data Breach, Plaintiff  
25 Villalon experienced two attempted unauthorized transactions on her PayPal account via her  
26 PayPal Cash Card. Said transactions were automatically declined because the transactions were  
27 more than what was in Plaintiff's account at that time.

1 22. Plaintiff Villalon is very concerned about additional identity theft, her banking  
2 account and fraud, as well as the consequences of such identity theft and fraud resulting from the  
3 Data Breach.

4 23. Plaintiff Villalon suffered actual injury from having Private Information  
5 compromised as a result of the Data Breach including, but not limited to (a) damage to and  
6 diminution in the value of her Private Information, a form of property that Defendant obtained  
7 from Plaintiff; (b) violation of Plaintiff's privacy rights; and (c) present and increased risk arising  
8 from the identity theft and fraud.

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

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

16 26. Defendant T-Mobile US, Inc. is a for-profit company incorporated in Delaware  
17 with its principal place of business in the State of Washington at 12920 SE 38th St, Bellevue,  
18 Washington 98006. Defendant is a wireless network operator and national telecommunications  
19 company that provides wireless voice and data services in the United States, Puerto Rico, and  
20 U.S. Virgin Islands. Defendant collects and maintains the personal information of millions of  
21 customers throughout the United States, including New York and Washington.

22 27. Defendant is a publicly traded company and in 2020, reported total revenue of  
23 \$68.4 billion.

## 24 VI. FACTUAL ALLEGATIONS

### 25 The Data Breach

26 28. On August 16, 2021, T-Mobile confirmed that it was the subject of a data breach  
27 affecting over 100 million customers. This acknowledgement came after a report by Vice.com on  
28

1 August 15, 2021, that an unidentified individual was attempting to sell PII from the T-Mobile  
2 server. The PII accessed in the data breach is believed to include customer's names, addresses,  
3 social security numbers, driver's license information, phone numbers, dates of birth, and unique  
4 IMEI and IMSI numbers. According to Vice.com, the unidentified individual knew T-Mobile  
5 became aware of the hack, because he or she eventually lost access to the backdoored servers.

6 29. On August 17, 2021, T-Mobile released a more detailed statement about the data  
7 breach, verifying that the hack did occur and how many customers were affected. Since August  
8 17, 2021, T-Mobile has identified over 10 million more customers whose PII was likely  
9 compromised.

10 30. On August 20, 2021, T-Mobile released another press statement, updating the  
11 number of customers likely affected by the data breach. T-Mobile also offered two years of free  
12 identity protection services with McAfee's ID Theft Protection Services and free scam-blocking  
13 protection through Scam Shield.

14 **The Value of Personally Identifiable Information**

15 31. PII, or personal identifiable information, is data that can be used to detect a  
16 specific individual. PII includes name, address, email, telephone number, date of birth, passport  
17 number, fingerprint, driver's license number, credit/debit card number, and social security  
18 number.

19 32. It is important to keep PII safe, especially in digital form. PII stored on a  
20 computer, phone, or website can be vulnerable to cybercriminals. If a criminal is fraudulently  
21 using a user's information, she can become the victim of fraud, identity theft, and/or phishing  
22 attacks.

23 **Defendant Was Aware of the Risks of a Data Breach**

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

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

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

6 36. Data breaches have become widespread. For example, the United States saw  
7 1,244 data breaches in 2018 and had 446.5 million exposed records.<sup>3</sup>

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

10 At T-Mobile, everyone is challenge[d] to think outside of  
11 conventional approaches to digital security; all know assumptions  
12 are reevaluated. We work on forward-thinking technologies,  
13 including micro-segmentation, machine learning, predictive  
14 analytics, web situational awareness, advance threat mitigation,  
15 active defense, data obfuscation and next-generation endpoint  
16 technologies it.<sup>4</sup>

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

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

24 40. According to the Federal Trade Commission ("FTC"), identity theft wreaks havoc  
25 on consumers' finances, credit history, and reputation and can take time, money, and patience to  
26 resolve.<sup>5</sup> Identity thieves use stolen personal information for a variety of crimes, including

27 <sup>3</sup> 98 Must-Know Data Breach Statistics for 2021, Varonis, <https://blogvaronis2.wpengin.com/data-breach-statistics/>  
28 (last visited Aug. 24, 2021).

<sup>4</sup> Digital Security, T-Mobile, <https://www.t-mobile.com/careers/digital-security> (last visited Aug. 24, 2021).

<sup>5</sup> 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. 24, 2021).

1 government benefits fraud, phone or utilities fraud, and bank and finance fraud.<sup>6</sup>

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

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

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

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

19 **Defendant Failed to Comply with FTC Security Guidelines on Storing and Protecting PII**

20 45. The FTC has promulgated numerous guides for businesses which highlight the  
21 importance of implementing reasonable data security practices. According to the FTC, the need  
22 for data security should be factored into all business decision-making.

23  
24 <sup>6</sup> *Id.* The FTC defines identity theft as “a fraud committed or attempted using the identifying information of another  
25 person without authority.” 16 CFR § 603.2. The FTC describes “identifying information” as “any name or number  
26 that may be used, alone or in conjunction with any other information, to identify a specific person,” including,  
27 among other things, “[n]ame, social security number, date of birth, official State or government issued driver's  
28 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.  
24, 2021).



1           46.     In 2016, the FTC updated its publication, Protecting Personal Information: A  
2 Guide for Business, which established cyber-security guidelines for businesses. The guidelines  
3 note that businesses should protect the personal customer information that they keep; properly  
4 dispose of personal information that is no longer needed; encrypt information stored on computer  
5 networks; understand their network’s vulnerabilities; and implement policies to correct any  
6 security problems. The guidelines also recommend that businesses use an intrusion detection  
7 system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating  
8 someone is attempting to hack the system; watch for large amounts of data being transmitted  
9 from the system; and have a response plan ready in the event of a breach.

10           47.     The FTC further recommends that companies not maintain Private Information  
11 longer than is needed for authorization of a transaction; limit access to sensitive data; require  
12 complex passwords to be used on networks; use industry-tested methods for security; monitor for  
13 suspicious activity on the network; and verify that third-party service providers have  
14 implemented reasonable security measures.

15           48.     The FTC has brought enforcement actions against businesses for failing to protect  
16 consumer data adequately and reasonably, treating the failure to employ reasonable and  
17 appropriate measures to protect against unauthorized access to confidential consumer data as an  
18 unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act (“FTCA”),  
19 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must  
20 take to meet their data security obligations.

21           49.     Defendant failed to properly implement basic data security practices, and their  
22 failure to employ reasonable and appropriate measures to protect against unauthorized access to  
23 consumer Private Information constitutes an unfair act or practice prohibited by Section 5 of the  
24 FTCA, 15 U.S.C. § 45. 67. Defendant was at all times fully aware of their obligation to protect  
25 the Private Information of current, former, and prospective customers. Defendant was also aware  
26 of the significant repercussions that would result from their failure to do so.

1 **Defendant Failed to Comply with Industry Standards**

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

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

11 52. Defendant failed to meet the minimum standards of the following cybersecurity  
12 frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation  
13 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,  
14 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  
15 for Internet Security's Critical Security Controls (CIS CSC), which are established standards in  
16 reasonable cybersecurity readiness.

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

20 **Plaintiff and Class Members Have Suffered Harm and Are at an Increased Risk of**  
21 **Fraud and Identity Theft as a Result of the Data Breach**

22 54. Due to the Data Breach, Plaintiff and Class members have suffered and will  
23 continue to suffer harm.

24 55. Plaintiff and Class members face an increased risk of identity theft, phishing  
25 attacks, and related cybercrimes because of the Data Breach. Those impacted are under  
26 heightened and prolonged anxiety, as they will be at risk for falling victim to cybercrimes for  
27 years to come.

1 56. As a result of the Data Breach, at least one unidentified cybercriminal possesses  
2 the PII of Plaintiff and Class members. Now that the data is stolen, unidentified actors can  
3 exploit the PII for their own gain or sell the PII to others for a profit. With social security  
4 numbers and driver's license information, cybercriminals can open new bank accounts and take  
5 out loans. Actions like these can destroy the Plaintiff and Class members' credit scores, having  
6 damage on future attempts to borrow money, obtain credit, or open a bank account.

7 57. Cybercriminals can also use breached PII to obtain medical treatment using  
8 victim's health insurance, file false federal and state tax returns, and obtain government benefits.  
9 Victims of such identity theft are targeted by the IRS, added to credit fraud watch lists, and can  
10 be barred from making major purchases such as a new car or home.

11 58. The PII obtained during the Data Breach is highly valuable to cybercriminals for  
12 the aforementioned reasons.

13 59. In response to the Data Breach, T-Mobile offered affected customer offered two  
14 years of free identity protection services with McAfee's ID Theft Protection Services. However,  
15 two years is not enough time to effectively monitor one's credit after identity theft.  
16 Cybercriminals will often wait months or years after obtaining PII to use it. Plaintiff and Class  
17 members will have to diligently monitor their credit for years after the complimentary McAfee  
18 ID Theft Protection Services are up in order to ensure their PII obtained in the Data Breach is not  
19 used to harm them.

20 **V. CLASS ACTION ALLEGATIONS**

21 60. Plaintiff brings this nationwide class action pursuant to rules 23(b)(2), 23(b)(3),  
22 and 23(c)(4) of the Federal Rules of Civil Procedure, individually and on behalf of all members  
23 of the following class:

24 All current, former, and prospective T-Mobile customers residing in  
25 the United States whose Private Information was compromised in  
26 the Data Breach announced by Defendant on or about August 16,  
27 2021 (the "Nationwide Class").

1           61. Plaintiff also brings this class action individually and on behalf of all people in  
2 New York defined as follows:

3                   All current, former, and prospective T-Mobile customers residing in  
4 New York whose personal information was compromised as a result  
5 of the breach of T-Mobile US, Inc.'s information system(s)  
6 announced by Defendant on August 16, 2021. (the "New York  
7 Subclass")

8           62. The New York Subclass is referred to herein as the "New York Subclass" and  
9 together with the Nationwide Class, are collectively referred to herein as the "Classes."

10           63. Excluded from the Classes is Defendant, any entities in which Defendant has a  
11 controlling interest or that have a controlling interest in Defendant, and Defendant's legal  
12 representatives, assignees and successors. Also excluded are all individuals who make a timely  
13 election to be excluded from this proceeding using the correct protocol for opting out, and all  
14 judges assigned to this case and their immediate family members and staff.

15           64. **Numerosity.** The Classes are so numerous that joinder of all members is  
16 impracticable. Upon information and belief, the Nationwide Class consists of over 46 million  
17 customers whose data was compromised in the data breach. Membership in the classes is  
18 identifiable in Defendant's records

19           65. **Commonality and Predominance.** There are numerous questions of law and fact  
20 common to Plaintiff and Class members. These common questions predominate over any  
21 questions affecting only individual members of the Classes. The common questions of law and  
22 fact include, without limitation:

- 23           a. When Defendant actually learned of the Data Breach and whether its  
24 response was adequate;
- 25           b. Whether Defendant owed a duty to the Classes to exercise due care in  
26 collecting, storing, safeguarding and/or obtaining their Private  
27 Information;
- 28           c. Whether Defendant breached that duty;

- 1 d. Whether Defendant implemented and maintained reasonable security
- 2 procedures and practices appropriate to the nature of storing the Private
- 3 Information of Plaintiff and Members of the Classes;
- 4 e. Whether Defendant knew or should have known that it did not employ
- 5 reasonable measures to keep the Private Information of Plaintiff and
- 6 Members of the Classes secure and to prevent loss or misuse of that
- 7 Private Information;
- 8 f. Whether Defendant adequately addressed and fixed the vulnerabilities
- 9 which permitted the Data Breach to occur;
- 10 g. Whether Defendant caused Plaintiff's and Members of the Classes
- 11 damage;
- 12 h. Whether Defendant violated the law by failing to promptly notify Plaintiff
- 13 and Members of the Classes that their Private Information had been
- 14 compromised;
- 15 i. Whether Defendant violated the consumer protection statutes invoked
- 16 below; and
- 17 j. Whether Plaintiff and the other Members of the Classes are entitled to
- 18 credit monitoring and other monetary relief.

19 66. **Typicality.** Plaintiff's claims are typical of the other Class Members because all  
20 members had Private Information compromised in the Data Breach and were harmed as a result.

21 67. **Adequacy.** Plaintiff will fairly and adequately represent and protect the interests  
22 of the Classes. Plaintiff has no interests that conflict with the interests of the Class she seeks to  
23 represent. Plaintiff's Counsel are competent and experienced in data breach class action  
24 litigation.

25 68. **Superiority.** A class action is superior to other available means of fair and  
26 efficient adjudication of the claims of Plaintiff and the Class. The injury suffered by each  
27 individual Class member is relatively small in comparison to the burden and expense of

1 individual prosecution of complex and expensive litigation. It would be very difficult, if not  
2 impossible, for members of the Class individually to effectively redress Defendant's  
3 wrongdoing. Even if Class members could afford such individual litigation, the court system  
4 could not. Individualized litigation presents a potential for inconsistent or contradictory  
5 judgments.

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

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

- 14 a. Whether Defendant owed a legal duty to Plaintiff and Members of the  
15 Classes to exercise due care in collecting, storing, using, and safeguarding  
16 their Private Information;
- 17 b. Whether Defendant breached a legal duty to Plaintiff and the Members of  
18 the Classes to exercise due care in collecting, storing, using, and  
19 safeguarding their Private Information;
- 20 c. Whether Defendant failed to comply with its own policies and applicable  
21 laws, regulations, and industry standards relating to data security;
- 22 d. Whether Defendant failed to implement and maintain reasonable security  
23 procedures and practices appropriate to the nature and scope of the  
24 information compromised in the Data Breach; and
- 25 e. Whether members of the Classes are entitled to actual damages, credit  
26 monitoring or other injunctive relief, and/or punitive damages as a result  
27 of Defendant's wrongful conduct.

1 **VI. FIRST CLAIM FOR RELIEF**

2 **Negligence**

3 **(On Behalf of Plaintiff, the Nationwide Class, and the New York Subclass)**

4 71. Plaintiff re-alleges and incorporates by reference herein all of the allegations  
5 contained in the preceding paragraphs.

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

9 73. The legal duties owed by Defendant to Plaintiff and Members of the Classes  
10 include, but are not limited to the following:

- 11 a. To exercise reasonable care in obtaining, retaining, securing, safeguarding,  
12 deleting, and protecting the Private Information of Plaintiff and Members  
13 of the Classes in its possession;
- 14 b. To protect Private Information of Plaintiff and Members of the Classes in  
15 its possession using reasonable and adequate security procedures that are  
16 compliant with industry-standard practices; and
- 17 c. To implement processes to quickly detect a data breach and to timely act  
18 on warnings about data breaches, including promptly notifying Plaintiff  
19 and Members of the Classes of the Data Breach.

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

25 75. Various FTC publications and data security breach orders further form the basis  
26 of Defendant's duty. Plaintiff and Members of the Classes are consumers under the FTC Act.  
27 Defendant violated Section 5 of the FTC Act by failing to use reasonable measures to protect  
28

1 Private Information and by not complying with industry standards.

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

6 77. Defendant knew or should have known that its security practices did not  
7 adequately safeguard the Private Information belonging to the Plaintiff and Members of the  
8 Classes.

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

15 79. Defendant breached the duties it owed to Plaintiff and Members of the Classes in  
16 several ways, including:

- 17 a. Failing to implement adequate security systems, protocols, and practices  
18 sufficient to protect current, former, and prospective customers' Private  
19 Information, including Plaintiffs and Members of the Classes, and thereby  
20 creating a foreseeable risk of harm;
- 21 b. Failing to comply with the minimum industry data security standards prior  
22 to the Data Breach; and
- 23 c. Failing to act despite knowing or having reason to know that its systems  
24 were vulnerable to attack.

25 80. Due to Defendant's conduct, Plaintiff and Members of the Classes are entitled to  
26 credit monitoring. Credit monitoring is reasonable here. The Private Information taken can be  
27 used for identity theft and other types of financial fraud against Plaintiff and Members of the  
28



1 Classes.

2 81. Some experts recommend that data breach victims obtain credit monitoring  
3 services for at least ten years following a data breach. Annual subscriptions for credit monitoring  
4 plans range from approximately \$219 to \$358 per year.<sup>7</sup>

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

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

21 **VII. SECOND CLAIM FOR RELIEF**

22 **Negligence Per Se**  
23 **(On Behalf of Plaintiff, the Nationwide Class, and the New York Subclass)**

24 84. Plaintiff re-alleges and incorporates by reference herein all of the allegations  
25 contained in the preceding paragraphs.

26 <sup>7</sup> In the recent Equifax data breach, for example, Equifax agreed to free monitoring of victims' credit reports at all  
27 three major credit bureaus for four years, plus \$1 million of identity theft insurance. For an additional six years,  
28 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.

1           85.       Section 5 of the FTC Act prohibits “unfair . . . practices in or affecting  
2 commerce,” including, as interpreted and enforced by the FTC, the unfair act or practice by  
3 businesses, such as Defendant’s, of failing to use reasonable measures to protect Private  
4 Information. The FTC publications and orders described above also form part of the basis of  
5 Defendant’s duty in this regard.

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

13           87.       Defendant’s violations of Section 5 of the FTC Act constitute negligence per se.

14           88.       Plaintiff and Members of the Classes are within the class of persons that the FTC  
15 Act was intended to protect.

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

21           90.       As a direct and proximate result of Defendant’s negligence per se, Plaintiff and  
22 Members Classes have suffered and will suffer injury, including but not limited to: (i) actual  
23 identity theft; (ii) the loss of the opportunity how their Private Information is used; (iii) the  
24 compromise, publication, and/or theft of their Private Information; (iv) out-of-pocket expenses  
25 associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or  
26 unauthorized use of their Private Information; (v) lost opportunity costs associated with effort  
27 expended and the loss of productivity addressing and attempting to mitigate the actual and future  
28

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

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

15 **VIII. THIRD CLAIM FOR RELIEF**

16 **Breach of Implied Contract**

17 **(On Behalf of Plaintiffs the Nationwide Class, and the New York Subclass)**

18 92. Plaintiff re-alleges and incorporates by reference herein all of the allegations  
19 contained in the preceding paragraphs.

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

24 94. Plaintiff and Class Members would not have provided their personal and financial  
25 information to Defendant, but for Defendant's implied promises to safeguard and protect  
26 Defendant's current, former, and prospective customers private personal and financial  
27 information.

1 95. Plaintiff and Class Members performed their obligations under the implied  
2 contract when they provided their private personal and financial information in exchange for  
3 telecommunication services provided by Defendant.

4 96. Defendant breached the implied contracts with Plaintiff and Class Members by  
5 failing to protect and keep private the nonpublic personal and financial information provided to  
6 them about Plaintiff and Class Members.

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

10 **IX. FOURTH CLAIM FOR RELIEF**  
11 **Violation of the Washington State Consumer Protection Act (RCW 19.86.010 et seq.)**  
12 **(On Behalf of Plaintiff and the Nationwide Class)**

13 98. Plaintiff re-alleges and incorporates by reference herein all of the allegations  
14 contained in the preceding paragraphs.

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

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

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

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

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

10           104. The gravity of Defendant’s wrongful conduct outweighs any alleged benefits  
11 attributable to such conduct. There were reasonably available alternatives to further Defendant’s  
12 legitimate business interests other than engaging in the above-described wrongful conduct.

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

23           106. Unless restrained and enjoined, Defendant will continue to engage in the above-  
24 described wrongful conduct and more data breaches will occur. Plaintiff, therefore, on behalf of  
25 herself, Class Members, and the general public, also seeks restitution and an injunction  
26 prohibiting Defendant from continuing such wrongful conduct, and requiring Defendant to  
27 modify their corporate culture and design, adopt, implement, control, direct, oversee, manage,  
28

1 monitor and audit appropriate data security processes, controls, policies, procedures protocols,  
2 and software and hardware systems to safeguard and protect the Private Information entrusted to  
3 it.

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

10 **X. FIFTH CLAIM FOR RELIEF**  
11 **Violation of the New York General Business Law §349**  
12 **(On behalf of Plaintiff, the Nationwide Class and the New York Class)**

13 108. Plaintiff re-alleges and incorporates by reference herein all of the allegations  
14 contained in the preceding paragraphs.

15 109. Defendant engaged in deceptive, unfair, and unlawful trade acts or practices in the  
16 conduct of trade or commerce and furnishing of services, in violation of N.Y. Gen. Bus. Law §  
17 349(a), including but not limited to the following:

- 18 a. Defendant misrepresented material facts to Plaintiff and Class members by  
19 representing that it would maintain adequate data privacy and security  
20 practices and procedures to safeguard Plaintiff's and Class members' PII  
21 from unauthorized disclosure, release, data breaches, and theft;
- 22 b. Defendant misrepresented material facts to Plaintiff and Class members by  
23 representing that it did and would comply with the requirements of federal  
24 and state laws pertaining to the privacy and security of Plaintiff's and  
25 Class members' PII;
- 26 c. Defendant omitted, suppressed, and concealed material facts of the  
27 inadequacy of its privacy and security protections for Plaintiff's and Class  
28

1 members' PII; and

2 d. Defendant engaged in deceptive, unfair, and unlawful trade acts or  
3 practices by failing to maintain the privacy and security of Plaintiff's and  
4 Class members' PII, in violation of duties imposed by and public policies  
5 reflected in applicable federal and state laws, resulting in the Data Breach.  
6 These unfair acts and practices violated duties imposed by laws including  
7 the Federal Trade Commission Act (15 U.S.C. § 45).

8 110. Defendant's failure constitutes false and misleading representations, which have  
9 the capacity, tendency, and effect of deceiving or misleading consumers (including Plaintiff and  
10 Class members) regarding the security of its network and aggregation of PII.

11 111. The misrepresentations upon which consumers (including Plaintiff and Class  
12 members) relied were material misrepresentations (e.g., as to Defendant's adequate protection of  
13 PII), and consumers (including Plaintiff and Class members) relied upon those representations to  
14 their detriment.

15 112. Defendant's conduct is unconscionable, deceptive, and unfair, as it is likely to,  
16 and did, mislead consumers acting reasonably under the circumstances. As a direct and  
17 proximate result of Defendant's conduct, Plaintiff and other Class members have been harmed,  
18 in that they were not timely notified of the data breach, which resulted in profound vulnerability  
19 to their personal information and other financial accounts.

20 113. As a direct and proximate result of Defendant's unconscionable, unfair, and  
21 deceptive acts and omissions, Plaintiff's and Class members' PII was disclosed to third parties  
22 without authorization, causing and will continue to cause Plaintiff and Class members damages.

23 114. As a direct and proximate result of Defendant's violation of NY GBL §349,  
24 Plaintiff and Class members have suffered, and continue to suffer, injuries, damages arising from  
25 identity theft; from their needing to contact governmental agencies; potentially defending  
26 themselves from legal action base upon fraudulent use of their PII; contacting their financial  
27 institutions; loss of use of funds; closing or modifying financial accounts; damages from lost  
28

1 time and effort to mitigate the actual and potential impact of the data breach on their lives;  
2 closely reviewing and monitoring their accounts for unauthorized activity which is certainly  
3 impending; placing credit freezes and credit alerts with credit reporting agencies; and damages  
4 from identity theft, which may take months or years to discover and detect.

5 **XI. SIXTH CLAIM FOR RELIEF**

6 **Unjust Enrichment**

7 **(On Behalf of Plaintiff, the Nationwide Class, and the New York Subclass)**

8 115. Plaintiff re-alleges and incorporates by reference herein all of the allegations  
9 contained in the preceding paragraphs.

10 116. Defendant benefited from receiving Plaintiff's and Members of the Classes'  
11 Private Information by its ability to retain and use that information for its own benefit. Defendant  
12 understood this benefit.

13 117. Defendant also understood and appreciated that Plaintiff's and Members of the  
14 Classes' Private Information was private and confidential, and its value depended upon  
15 Defendant maintaining the privacy and confidentiality of that Private Information.

16 118. Plaintiff's and Members of the Classes who were customers of Defendant's  
17 customer conferred a monetary benefit upon Defendant in the form of monies paid for services  
18 available from Defendant.

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

23 120. The monies that Plaintiff's and Members of the Classes paid to Defendant for  
24 services were to be used by Defendant, in part, to pay for the administrative costs of reasonable  
25 data privacy and security practices and procedures.

26 121. Defendant also understood and appreciated that Plaintiff's and Members of the  
27 Classes' Private Information was private and confidential, and its value depended upon  
28



1 Defendant maintaining the privacy and confidentiality of that Private Information.

2 122. But for Defendant's willingness and commitment to maintain privacy and  
3 confidentiality, that Private Information would not have been transferred to and entrusted with  
4 Defendant. Indeed, if Defendant had informed Plaintiff's and Members of the Classes that their  
5 data and cyber security measures were inadequate, Defendant would not have been permitted to  
6 continue to operate in that fashion by regulators, its shareholders, and its consumers.

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

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

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

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

26 127. Defendant should be compelled to disgorge into a common fund for the benefit of  
27 Plaintiff's and Members of the Classes all unlawful or inequitable proceeds they received as a  
28

1 result of the conduct alleged herein.

2 **XII. PRAYER FOR RELIEF**

3 WHEREFORE, Plaintiff prays for judgment against Defendant as follows:

4 A. Certification of the Classes pursuant to Federal Rule of Civil Procedure 23;

5 B. Appoint Plaintiff Ania Villalon as representative of the Classes;

6 C. Appoint the undersigned counsel as counsel for the Classes;

7 D. That the Court award compensatory damages, punitive damages, statutory and  
8 civil penalties to Plaintiff and the Classes as warranted by all applicable laws alleged herein;

9 E. In the alternative, that the Court award nominal damages as permitted by law;

10 F. That the Court award injunctive or other equitable relief that directs Defendant to  
11 provide Plaintiff and the Classes with free credit monitoring and identity theft protection, and to  
12 implement reasonable security procedures and practices to protect customers' PII that conform to  
13 relevant federal and state guidelines and industry norms;

14 G. That the Court award declaratory judgment in favor of Plaintiff determining that  
15 Defendant's failure to implement reasonable security measures gives rise to a claim under the  
16 laws alleged herein;

17 H. Award Plaintiff and the Classes statutory, compensatory and exemplary damages  
18 as permitted by law;

19 I. Judgment against Defendant for attorney's fees and costs as permitted by law  
20 and/or equity;

21 J. Any other or further relief which the Court deems fair and equitable.

22 **XIII. DEMAND FOR JURY TRIAL**

23 Pursuant to Fed. R. Civ. P. 38(b), Plaintiff demands a trial by jury of all issues properly  
24 triable to a jury in this case.

1 RESPECTFULLY SUBMITTED AND DATED this 24th day of August, 2021

2  
3 TERRELL MARSHALL LAW GROUP PLLC

4 By: /s/ Beth E. Terrell, WSBA #26759  
5 Beth E. Terrell, WSBA #26759  
6 Email: bterrell@terrellmarshall.com  
7 936 N. 34th Street, Suite 300  
8 Seattle, Washington 98103  
9 Telephone: (206) 206-816-6603  
10 Facsimile: (206) 319-5450

11 Kevin Laukaitis\*  
12 Email: klaukaitis@shublawyers.com  
13 Jonathan Shub\*  
14 Email: jshub@shublawyers.com  
15 SHUB LAW FIRM LLC  
16 134 Kings Highway East, 2<sup>nd</sup> Floor  
17 Haddonfield, New Jersey 08033  
18 Telephone: (856) 772-7200  
19 Facsimile: (856) 210-9088

20 *Attorneys for Plaintiff and the Classes*

21 *\*Pro hac vice forthcoming*