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

STEPHANIE PERALTA, BRIAN GRADY, AND MICHAEL JONES, individually and on behalf of all similarly situated persons and on behalf of the general public, Plaintiffs, v. T-MOBILE USA, INC. Defendant.	Case No. CIV-21-838-HE **CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

Plaintiffs, Stephanie Peralta, Brian Grady, and Michael Jones, individually and on behalf of all others similarly situated, and on behalf of the general public, upon personal knowledge of facts pertaining to them and upon information and belief as to all other matters, and by and through undersigned counsel, hereby bring this Class Action Complaint against Defendant, T-Mobile USA, Inc. ("T-Mobile"), and allege as follows:

INTRODUCTION

1. Part of the bargain of purchasing a phone and/or services from T-Mobile includes turning over valuable personally identifiable information ("PII"),[1] including

[1] Personally identifiable information generally incorporates information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information. 2 CFR § 200.79. At a minimum, it includes all information that on its face expressly identifies an individual. PII is also generally defined to include certain identifiers that do not on their face name an individual, but that are considered to be particularly sensitive and/or valuable if in the wrong hands (for example, Social Security number, passport number, driver's license number, or financial account number).

names, address, Social Security numbers, birth dates, and driver's license information. If left unprotected, identity thieves can gain access to and use this highly sensitive information to fraudulently open new accounts, access existing accounts, perpetrate identity fraud or impersonate victims in a myriad of schemes, all of which can cause grievous financial harm, negatively affect the victim's credit scores for years, and cause victims to spend countless hours mitigating damage.

2. Every year millions of Americans have their most valuable PII stolen and sold online because of data breaches. Despite the dire warnings about the severe impact of data breaches on Americans of all economic strata, companies still fail to make the necessary investments to implement important and adequate security measures to protect their customers' and employees' data.

3. T-Mobile, a subsidiary of Deutsche Telekom AG, is one of the world's largest mobile telecommunications companies. T-Mobile is among those companies that have failed to meet their obligation to protect sensitive PII entrusted to them by their current and former customers.

4. As reported by T-Mobile, hackers found their way into T-Mobile's systems, stealing both former and current customer names, birth dates, Social Security numbers and driver's license information of T-Mobile (the "Data Breach").

5. The Data Breach is the fourth breach of T-Mobile's systems since early 2020, and the third in less than a year.[2]

[2] *See* https://www.tomsguide.com/news/possible-t-mobile-data-breach (last accessed August 19, 2021).

6. The cybercriminals responsible for this latest attack began offering Plaintiffs' and Class Members'[3] stolen PII for sale the weekend of August 14-15, 2021, according to security researcher Brian Krebs, who predicted that "it would all wind up online soon."[4]

7. Defendant T-Mobile required its customers to provide it with their sensitive PII and failed to protect it. Defendant had an obligation to secure its customers' PII by implementing reasonable and appropriate data security safeguards. This was part of the bargain between Plaintiffs and Class Members and T-Mobile.

8. As a result of T-Mobile's failure to provide reasonable and adequate data security, Plaintiffs' and the Class Members' unencrypted, non-redacted PII has been exposed to unauthorized third parties. Plaintiffs and the Class are now at much higher risk of identity theft and cybercrimes of all kinds, especially considering the highly sensitive PII stolen here and the fact that the compromised PII is already being sold on the dark web. This risk constitutes a concrete injury suffered by Plaintiffs and the Class, as they no longer have control over their PII, which PII is now in the hands of third-party cybercriminals. This substantial and imminent risk of identity theft has been recognized by numerous courts as a concrete injury sufficient to establish standing.[5]

---

[3] As used herein, the terms "Class" or "Class Members" means the putative "Nationwide Class" and "Oklahoma Subclass" defined herein.

[4] *See* https://www.latimes.com/business/technology/story/2021-08-18/how-to-protect-yourself-in-t-mobile-hack (last accessed August 19, 2021).

[5] *See, e.g., Resnick v. AvMed, Inc*., 693 F.3d 1317, 1324 (11th Cir. 2012) (holding that the misuse of plaintiff's sensitive information to open a bank account was sufficient to confer standing even where she did not allege any "unreimbursed losses"); *Galaria v. Nationwide Mut. Ins. Co.,* 663 F. App'x 384, 388 (6th Cir. 2016) (finding injury-in-fact for data breach case and defining "actual misuse" as a "fraudulent charge"); *Hutton v. Nat'l Bd. of Exam'rs in Optometry, Inc.*, 892 F.3d 613, 622 (4th Cir. 2018) (standing conferred based on alleged

9. Furthermore, Plaintiffs and the Class, as also set forth below, will have to incur costs to pay a third-party credit and identity theft monitoring service for the rest of their lives as a direct result of the Data Breach.

THE PARTIES

10. Defendant T-Mobile, a publicly traded company and subsidiary of Deutsche Telekom, is headquartered in Bellevue, Washington, is one of the mobile telecommunication industries' most recognizable brands in the world.

11. T-Mobile is the second-largest wireless carrier in the United states, with almost 105 million customers as of the end of Q2 2021. Of those 105 million customers, roughly 48 million were affected by the Data Breach.[6]

12. Plaintiff Peralta is a resident of Oklahoma County, Oklahoma and applied for credit to purchase a phone through T-Mobile.

13. Plaintiff Grady is a resident of Cleveland County, Oklahoma and has been a

---

fraudulent use of identifying information, without alleged unreimbursed expenses, because "the Supreme Court long ago made clear that 'in interpreting injury in fact ... standing [is] not confined to those who [can] show economic harm.'"); *In re Equifax, Inc. Customer Data Security Breach Litigation*, No. 20-10249, 2021 WL 2250845, at *6 (11th Cir. June 3, 2021) (holding that the plaintiffs plausibly alleged injury in fact and established standing "given the colossal amount of sensitive data stolen, including Social Security numbers, names, and dates of birth, and the unequivocal damage that can be done with this type of data…"); *McMorris v. Carlos Lopez & Associates, LLC*, 995 F.3d 295 (2d Cir. 2021) (recognizing that plaintiffs may establish Article III standing based on an increased risk of identity theft or fraud following the unauthorized disclosure of their data); *Attias v. Carefirst, Inc.*, 865 F.3d 620, 628-29 (D.C. Cir. 2017) ("The principal question, then, is whether the plaintiffs have plausibly alleged a risk of future injury that is substantial enough to create Article III standing. We conclude that they have.").

[6] *See* https://www.latimes.com/business/technology/story/2021-08-18/how-to-protect-yourself-in-t-mobile-hack (last accessed August 19, 2021).

customer of T-Mobile for over ten (10) years.

14. Plaintiff Jones is a resident of Oklahoma County, Oklahoma and has been a T-Mobile customer for approximately five (5) years.

15. Plaintiffs all provided their PII to T-Mobile at T-Mobile's request. Plaintiffs reasonably believed T-Mobile would keep their PII secure. Had T-Mobile disclosed to Plaintiffs that their PII would not be kept secure and would be easily accessible to criminal hackers and third parties and later sold on the dark web as a result, they would have demanded T-Mobile take additional precautions relating to their PII.

JURISDICTION AND VENUE

16. Subject matter jurisdiction in this civil action is authorized pursuant to 28 U.S.C. § 1332(d) because there are more than 100 Class Members, at least one class member is a citizen of a state different from that of Defendant, and the amount in controversy exceeds $5 million, exclusive of interest and costs.

17. This Court has personal jurisdiction over Defendant because it is registered to conduct business in Oklahoma and has sufficient minimum contacts with Oklahoma.

18. Venue is likewise proper in this District pursuant to 28 U.S.C. § 1391(b) because Defendant conducts much of its business in this District and Defendant has caused harm to Class Members residing in this District.

FACTUAL ALLEGATIONS

A. T-Mobile collects and stores millions of current and former customers' PII and has failed to provide adequate data security to protect it.

19. T-Mobile, which is headquartered in Washington with locations in

Oklahoma, is the second-largest wireless carrier in the United States and has annual revenues over $40 billion.[7]

20. Currently T-Mobile, a publicly traded company, has millions of current and former customers, and is also well-recognized brand on the mobile telecommunications global stage. T-Mobile touts on its website that its privacy principles mean "you can trust us to do the right thing with your data."[8]

B. T-Mobile's inadequate data security exposed its current and former customers' sensitive PII.

21. On August 17, 2021, T-Mobile learned that a bad actor gained access to T-Mobile's systems where highly sensitive customer data was being contained unencrypted.

22. Plaintiffs received Data Breach notices in the form of text messages from T-Mobile (collectively, the "Notice").

23. The Notice was sent to Plaintiffs via text message. T-Mobile also posted a separate notification of the Data Breach on its website, which included the following information:

> **What happened:**
>
> On August 17, 2021, 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. The latest details about the affected data are available here.
>
> **Information involved:**

[7] *See* https://www.statista.com/statistics/219435/total-revenue-of-t-mobile-usa-by-quarter/ (last accessed August 19, 2021)
[8] *See* https://www.t-mobile.com/privacy-center (last accessed August 19, 2021).

> Our investigation is ongoing and this information may be updated. The exact personal information accessed varies by individual. We have determined that the types of impacted information include: names, drivers' licenses, government identification numbers, Social Security numbers, dates of birth, T-Mobile prepaid PINs (which have already been reset to protect you), addresses and phone number(s). We have no indication that personal financial or payment information, credit or debit card information, account numbers, or account passwords were accessed.
>
> **What we're doing:**
>
> We're relentlessly focused on taking care of our customers – that has not changed. We've been working around the clock to address this event and continue protecting you, which includes taking immediate steps to protect all individuals who may be at risk.

24. After receiving the Notice, it is reasonable for recipients, including Plaintiffs and Class Members, to believe that the risk of future harm (including identity theft) is substantial and imminent, especially considering it has already been confirmed that Plaintiff's and Class Members' PII has been made available for sale on the dark web.

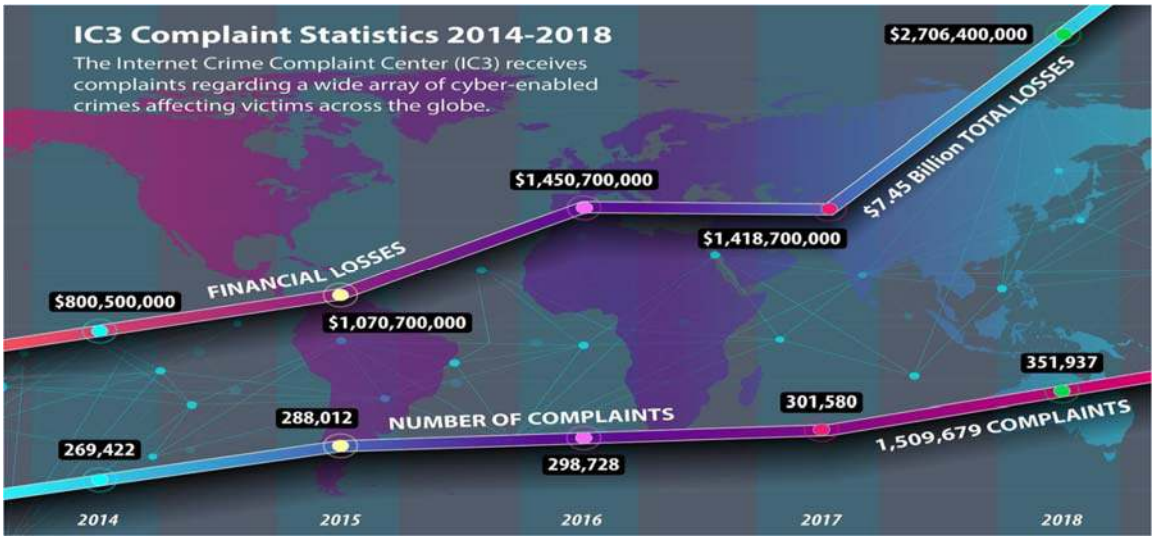
25. As such, it is also reasonable for Plaintiffs and Class Members to take steps to mitigate that substantial risk of future harm. In fact, in T-Mobile's online notification to its customers, it warns affected individuals of the potential misuse of their information and that they should, among other things, remain vigilant in reviewing their financial account statements and credit reports for fraudulent or irregular activity, and be alert for phishing emails.[9]

C. The PII exposed by T-Mobile as a result of its inadequate data security is highly valuable on the black market.

[9] *See* https://www.t-mobile.com/support/account/additional-steps-to-protect-yourself?icid=MGPO_MTW_U_21DTASECRT_SVFBJIM81C0IT0Q26102 (last accessed August 20, 2021).

26. The information exposed by T-Mobile is a virtual goldmine for phishers, hackers, identity thieves and cyber criminals.

27. This exposure, along with the fact that the compromised PII is already being sold on the dark web, is tremendously problematic. Cybercrime is rising at an alarming rate, as shown in the FBI's Internet Crime Complaint statistics chart shown below:



28. By 2013, it was being reported that nearly one out of four data breach notification recipients becomes a victim of identity fraud.[10]

29. Stolen PII is often trafficked on the dark web, as is the case here. Law enforcement has difficulty policing the dark web due to this encryption, which allows users and criminals to conceal identities and online activity.

30. When malicious actors infiltrate companies and copy and exfiltrate the PII that those companies store, that stolen information often ends up on the dark web because the malicious actors buy and sell that information for profit.[11]

---

[10] Pascual, Al, "2013 Identity Fraud Report: Data Breaches Becoming a Treasure Trove for Fraudsters," *Javelin* (Feb. 20, 2013).

[11] *Shining a Light on the Dark Web with Identity Monitoring*, IdentityForce, Dec. 28,

31. For example, when the U.S. Department of Justice announced its seizure of AlphaBay in 2017, AlphaBay had more than 350,000 listings, many of which concerned stolen or fraudulent documents that could be used to assume another person's identity. Other marketplaces, similar to the now-defunct AlphaBay, "are awash with [PII] belonging to victims from countries all over the world. One of the key challenges of protecting PII online is its pervasiveness. As data breaches in the news continue to show, PII about employees, customers and the public is housed in all kinds of organizations, and the increasing digital transformation of today's businesses only broadens the number of potential sources for hackers to target."[12]

32. The PII of consumers 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[13]. Experian reports that a stolen credit or debit card number can sell for $5 to $110 on the dark web[14].

2020, *available at:* https://www.identityforce.com/blog/shining-light-dark-web-identity-monitoring (last accessed July 28, 2021).

[12] *Stolen PII & Ramifications: Identity Theft and Fraud on the Dark Web*, Armor, April 3, 2018, *available at:* https://www.armor.com/resources/blog/stolen-pii-ramifications-identity-theft-fraud-dark-web/ (last accessed July 28, 2021).

[13] *Your personal data is for sale on the dark web. Here's how much it costs,* Digital Trends, Oct. 16, 2019, *available at*: https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/ (last accessed July 28, 2021).

[14] *Here's How Much Your Personal Information Is Selling for on the Dark Web*, Experian, Dec. 6, 2017, *available at*: https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/ (last accessed July 28, 2021).

Criminals can also purchase access to entire company data breaches from $900 to $4,500[15].

33. 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 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:

> 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[16].

34. 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.

35. 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

---

[15] *In the Dark*, VPNOverview, 2019, *available at*: https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/ (last accessed July 28, 2021).

[16] Social Security Administration, *Identity Theft and Your Social Security Number*, *available at*: https://www.ssa.gov/pubs/EN-05-10064.pdf (last visited July 28, 2021).

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."[17]

36. Because of this, the information compromised in the Data Breach here is significantly more harmful to lose than the loss of, for example, credit card information in a retailer payment card breach because victims can simply 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.

37. The PII compromised in the Data Breach 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 10 times on the black market."[18]

38. Once PII is sold, it is often used to gain access to various areas of the victim's digital life, including bank accounts, social media, credit card, and tax details. This can lead to additional PII being harvested from the victim, as well as PII from family, friends and colleagues of the original victim.

39. According to the FBI's Internet Crime Complaint Center (IC3) 2019 Internet Crime Report, Internet-enabled crimes reached their highest number of complaints and

---

[17] Bryan Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR (Feb. 9, 2015), *available at*: http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millionsworrying-about-identity-theft (last visited July 28, 2021).

[18] Time Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, IT World, (Feb. 6, 2015), *available at*: https://www.networkworld.com/article/2880366/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html (last visited July 28, 2021).

dollar losses in 2019, resulting in more than $3.5 billion in losses to individuals and business victims.

40. Victims of identity theft also often suffer embarrassment, blackmail, or harassment in person or online, and/or experience financial losses resulting from fraudulently opened accounts or misuse of existing accounts.

41. Data breaches facilitate identity theft as hackers obtain consumers' PII and thereafter use it to siphon money from current accounts, open new accounts in the names of their victims, or sell consumers' PII to others who do the same.

42. For example, the United States Government Accountability Office noted in a June 2007 report on data breaches (the "GAO Report") that criminals use PII to open financial accounts, receive government benefits, and make purchases and secure credit in a victim's name.[19] The GAO Report further notes that this type of identity fraud is the most harmful because it may take some time for a victim to become aware of the fraud, and can adversely impact the victim's credit rating in the meantime. The GAO Report also states that identity theft victims will face "substantial costs and inconveniences repairing damage to their credit records . . . [and their] good name."[20]

43. The exposure of Plaintiffs' and Class Members' PII to cybercriminals will continue to cause substantial risk of future harm (including identity theft) that is continuing

[19] *See* Government Accountability Office, *Personal Information: Data Breaches are Frequent, but Evidence of Resulting Identity Theft is Limited; However, the Full Extent is Unknown* (June 2007), https://www.gao.gov/assets/gao-07-737.pdf (last visited July 28, 2021).
[20] *Id.*

and imminent in light of the many different avenues of fraud and identity theft utilized by third-party cybercriminals to profit off of this highly sensitive information.

D. T-Mobile Failed to Comply with Federal Trade Commission Requirements.

44. Federal and State governments have established security standards and issued recommendations to minimize data breaches and the resulting harm to individuals and financial institutions. The Federal Trade Commission ("FTC") has issued numerous guides for businesses that highlight the importance of reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.[21]

45. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established guidelines for fundamental data security principles and practices for business.[22] Among other things, the guidelines note businesses should 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 correct 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

[21] *See* Federal Trade Commission, *Start With Security* (June 2015), https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf (last visited July 28, 2021).

[22] *See* Federal Trade Commission, *Protecting Personal Information: A Guide for Business* (Oct. 2016), https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last visited July 28, 2021).

event of a breach.[23]

46. Additionally, the FTC recommends that companies 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.[24]

47. Highlighting the importance of protecting against phishing and other types of data breaches, the FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect PII, 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 ("FTC Act"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.[25]

48. By negligently securing Plaintiffs' and Class Members' PII and allowing an unknown third-party cybercriminal to access T-Mobile systems for a fourth time in two years in order to access unencrypted customers' PII, T-Mobile failed to employ reasonable and appropriate measures to protect against unauthorized access to confidential customer data. T-Mobile's data security policies and practices constitute unfair acts or practices prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

---

[23] *Id.*

[24] Federal Trade Commission, *Start With Security*, *supra footnote 17*.

[25] Federal Trade Commission, *Privacy and Security Enforcement Press Releases*, https://www.ftc.gov/news-events/media-resources/protecting-consumer-privacy/privacy-security-enforcement (last visited July 28, 2021).

E. Plaintiff Peralta's Experience

49. Plaintiff Peralta applied for credit with T-Mobile to purchase a phone.

50. After applying for credit with T-Mobile, Plaintiff Peralta decided to remain with her previous mobile phone carrier instead of switching to T-Mobile.

51. In late-July of 2021, Plaintiff Peralta began having problems with her credit report, which showed a $1,000.00 debt to T-Mobile for a phone she did not purchase.

52. On or around August 19, 2021, Plaintiff Peralta learned about the T-Mobile Data Breach.

53. Plaintiff Peralta now believes the problem she is having with her credit report may be the result of the data breach.

54. Plaintiff Peralta believes her PII is now being sold on the dark web.

55. As a direct and traceable result of the Data Breach, Plaintiff Peralta has been forced to spend time dealing with and responding to the direct consequences of the Data Breach, which include spending time on the telephone and sorting through unsolicited emails, researching the Data Breach, exploring credit monitoring and identity theft insurance options, and self-monitoring her accounts. This is time that has been lost forever and cannot be recaptured.

56. Plaintiff Peralta is very careful about sharing her PII. She has never knowingly transmitted unencrypted PII over the internet or any other unsecured source.

57. Plaintiff Peralta stores all documents containing her PII in a safe and secure location. Moreover, she diligently chooses unique usernames and passwords for the few online accounts that she has.

58. Plaintiff Peralta has suffered actual, concrete injury in the form of damages to, and diminution in, the value of her PII – a form of intangible property that Plaintiff Peralta entrusted to Defendant to purchase Defendant's products and services. This PII was compromised in, and has been diminished as a result of, the Data Breach.

59. Plaintiff Peralta has also suffered actual, concrete injury in the forms of lost time and opportunity costs, annoyance, interference, and inconvenience as a direct and traceable result of the Data Breach, and has stress, anxiety and increased concerns due to the loss of her privacy and the substantial risk of fraud and identity theft which she now faces as her PII is being sold on the dark web.

60. Plaintiff Peralta has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse of her PII resulting from the compromise of her PII, especially her Social Security number and driver's license information, in combination with her full name, which PII is now in the hands of cyber criminals and other unauthorized third parties and being sold on the dark web.

61. Knowing that thieves stole her PII, including her Social Security Number and driver's license number, along with the other PII she was required to provide to T-Mobile, and knowing that her PII is now being sold on the dark web, has caused Plaintiff Peralta great anxiety.

62. Additionally, Plaintiff Peralta has never knowingly transmitted unencrypted PII over the internet or any other unsecured source. She deletes any and all electronic documents containing her PII and destroys any documents that may contain any of her PII, or that may contain any information that could otherwise be used to compromise her PII.

63. Plaintiff Peralta has a continuing interest in ensuring that her PII which, upon information and belief, remains in the possession of Defendant, is protected and safeguarded from future data breaches, especially considering Defendant's recent history of data breaches.

64. As a direct and traceable result of the Data Breach, Plaintiff Peralta will continue to be at heightened risk for financial fraud, identity theft, other forms of fraud, and the attendant damages, for years to come and will have to pay an identity monitoring company for the rest of her life to protect her exposed PII.

F. Plaintiff Grady's Experience

65. Plaintiff Grady became a T-Mobile customer over ten (10) years ago.

66. On or around August 20, 2021, Plaintiff Grady received the Notice from T-Mobile informing him of the Data Breach.

67. Upon information and belief, Mr. Grady's PII is now being sold on the dark web.

68. As a direct and traceable result of the Data Breach, Plaintiff Grady has been forced to spend time dealing with and responding to the direct consequences of the Data Breach, which include researching the Data Breach, exploring credit monitoring and identity theft insurance options, and self-monitoring his accounts. This is time that has been lost forever and cannot be recaptured.

69. Plaintiff Grady is careful about sharing his PII. He has never knowingly transmitted unencrypted PII over the internet or any other unsecured source.

70. Plaintiff Grady stores all documents containing his PII in a safe and secure

location. Moreover, he diligently chooses unique usernames and passwords for the online accounts that he has.

71. Plaintiff Grady has suffered actual, concrete injury in the form of damages to, and diminution in, the value of his PII – a form of intangible property that Plaintiff Grady entrusted to Defendant to purchase Defendant's products and services. This PII was compromised in, and has been diminished as a result of, the Data Breach.

72. Plaintiff Grady has also suffered actual, concrete injury in the forms of lost time and opportunity costs, annoyance, interference, and inconvenience as a direct and traceable result of the Data Breach, and has stress, anxiety and increased concerns due to the loss of his privacy and the substantial risk of fraud and identity theft which he now faces as his PII is being sold on the dark web.

73. Plaintiff Grady has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse of his PII resulting from the compromise of his PII, especially his Social Security number and driver's license information, in combination with his full name, which PII is now in the hands of cyber criminals and other unauthorized third parties and being sold on the dark web.

74. Knowing that thieves stole his PII, including his Social Security Number and driver's license number, along with the other PII he was required to provide to T-Mobile, and knowing that his PII is now being sold on the dark web, has caused Plaintiff Grady great anxiety.

75. Additionally, Plaintiff Grady has never knowingly transmitted unencrypted PII over the internet or any other unsecured source. He deletes any and all electronic

documents containing his PII and destroys any documents that may contain any of his PII, or that may contain any information that could otherwise be used to compromise his PII.

76. Plaintiff Grady has a continuing interest in ensuring that his PII which, upon information and belief, remains in the possession of Defendant, is protected and safeguarded from future data breaches, especially considering Defendant's recent history of data breaches.

77. As a direct and traceable result of the Data Breach, Plaintiff Grady will continue to be at heightened risk for financial fraud, identity theft, other forms of fraud, and the attendant damages, for years to come and will have to pay an identity monitoring company for the rest of his life to protect his exposed PII.

G. Plaintiff Jones's Experience

78. Plaintiff Jones became a T-Mobile customer in or about the year 2016.

79. On or around August 20, 2021, Plaintiff Jones received the Notice from T-Mobile informing him of the Data Breach.

80. Upon information and belief, Mr. Jones's PII is now being sold on the dark web.

81. As a direct and traceable result of the Data Breach, Plaintiff Jones has been forced to spend time dealing with and responding to the direct consequences of the Data Breach, which include spending time on the telephone and sorting through unsolicited emails, researching the Data Breach, exploring credit monitoring and identity theft insurance options, and self-monitoring his accounts. This is time that has been lost forever and cannot be recaptured.

82. Plaintiff Jones is very careful about sharing his PII. He has never knowingly transmitted unencrypted PII over the internet or any other unsecured source.

83. Plaintiff Jones stores all documents containing his PII in a safe and secure location. Moreover, he diligently chooses unique usernames and passwords for the online accounts that he has.

84. Plaintiff Jones has suffered actual, concrete injury in the form of damages to, and diminution in, the value of his PII – a form of intangible property that Plaintiff Jones entrusted to Defendant to purchase Defendant's products and services. This PII was compromised in, and has been diminished as a result of, the Data Breach.

85. Plaintiff Jones has also suffered actual, concrete injury in the forms of lost time and opportunity costs, annoyance, interference, and inconvenience as a direct and traceable result of the Data Breach, and has stress, anxiety and increased concerns due to the loss of his privacy and the substantial risk of fraud and identity theft which he now faces as his PII is being sold on the dark web.

86. Plaintiff Jones has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse of his PII resulting from the compromise of his PII, especially his Social Security number and driver's license information, in combination with his full name, which PII is now in the hands of cyber criminals and other unauthorized third parties and being sold on the dark web.

87. Knowing that thieves stole his PII, including his Social Security Number and driver's license number, along with the other PII he was required to provide to T-Mobile, and knowing that his PII is now being sold on the dark web, has caused Plaintiff Jones

great anxiety.

88. Additionally, Plaintiff Jones has never knowingly transmitted unencrypted PII over the internet or any other unsecured source. He deletes any and all electronic documents containing his PII and destroys any documents that may contain any of his PII, or that may contain any information that could otherwise be used to compromise his PII.

89. Plaintiff Jones has a continuing interest in ensuring that his PII which, upon information and belief, remains in the possession of Defendant, is protected and safeguarded from future data breaches, especially considering Defendant's recent history of data breaches.

90. As a direct and traceable result of the Data Breach, Plaintiff Jones will continue to be at heightened risk for financial fraud, identity theft, other forms of fraud, and the attendant damages, for years to come and will have to pay an identity monitoring company for the rest of his life to protect his exposed PII.

H. Plaintiffs and the Class Members suffered damages.

91. The ramifications of Defendant's failure to keep current and former customers' PII secure are long lasting and severe. Once PII is stolen, fraudulent use of that information and damage to victims may continue for years.[26]

92. The PII belonging to Plaintiffs and Class Members is private, sensitive in nature, and was left inadequately protected by Defendant who did not obtain Plaintiffs' or

[26] *2014 LexisNexis True Cost of Fraud Study, available at:* https://www.lexisnexis.com/risk/downloads/assets/true-cost-fraud-2014.pdf (last accessed July 28, 2021).

Class Members' consent to disclose such PII to any other person as required by applicable law and industry standards.

93. Defendant required Plaintiffs and Class Members to provide it with their PII, including full names and Social Security numbers. Implied in these exchanges was a promise by Defendant to ensure that the PII of Plaintiffs and Class Members in its possession was only used to provide the agreed-upon products and services being offered by Defendant.

94. Plaintiffs and Class Members, therefore, did not receive the benefit of the bargain with Defendant, because providing their PII to Defendant was in exchange for Defendant's agreement to secure it and keep it safe.

95. The Data Breach was a direct and proximate result of T-Mobile's failure to: (a) properly safeguard and protect Plaintiffs' and Class Members' PII from unauthorized access, use, and disclosure, as required by various state and federal regulations, industry practices, and common law; (b) establish and implement appropriate administrative, technical, and physical safeguards to ensure the security and confidentiality of Plaintiffs' and Class Members' PII; and (c) protect against reasonably foreseeable threats to the security or integrity of such information.

96. Defendant had the resources necessary to prevent the Data Breach, but neglected to implement adequate data security measures, despite its obligations to protect current and former customers' PII, and despite its public statements and representations that T-Mobile would keep their PII safe.

97. Had Defendant remedied the deficiencies in its data security systems and

protocols and adopted security measures recommended by experts in the field, it would have prevented the intrusion leading to the theft of PII.

98. As a direct and proximate result of Defendant's wrongful actions and inactions, Plaintiffs and Class Members have been placed at an imminent, immediate, and continuing increased risk of harm from identity theft and fraud, requiring them to take the time which they otherwise would have dedicated to other life demands such as work and family in an effort to mitigate the actual and potential impact of the Data Breach on their lives.

99. The U.S. Department of Justice's Bureau of Justice Statistics found that "among victims who had personal information used for fraudulent purposes, 29% spent a month or more resolving problems" and that "resolving the problems caused by identity theft [could] take more than a year for some victims."[27]

100. As a direct result of the Defendant's failures to prevent the Data Breach, Plaintiffs and Class Members have suffered, will suffer, and are at increased risk of suffering:

a. The compromise, publication, theft, and/or unauthorized use of their PII;

b. Out-of-pocket costs associated with the prevention, detection, recovery, and remediation from identity theft or fraud;

[27] U.S. Department of Justice, Office of Justice Programs Bureau of Justice Statistics, *Victims of Identity Theft, 2012*, December 2013, *available at*: https://www.bjs.gov/content/pub/pdf/vit12.pdf (last accessed July 28, 2021).

c. Lost opportunity costs and lost wages associated with efforts expended and the loss of productivity from addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft and fraud;

d. The continued risk to their PII, which remains in the possession of Defendant and is subject to further breaches so long as Defendant continues to fail to undertake appropriate measures to protect the PII in its possession; and

e. Current and future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, remediate, and repair the impact of the Data Breach for the remainder of the lives of Plaintiffs and Class Members.

101. In addition to a remedy for the economic harm, Plaintiffs and Class Members maintain an undeniable interest in ensuring that their PII is secure, remains secure, and is not subject to further misappropriation and theft, especially considering Defendant's recent history of data breaches.

102. To date, other than providing a woefully inadequate twenty-four (24) months of credit monitoring and identity protection services, Defendant does not appear to be taking any measures to assist Plaintiffs and Class Members.

103. Defendant's failure to adequately protect Plaintiffs' and Class Members' PII has resulted in Plaintiffs and Class Members having to undertake tasks requiring extensive amounts of time, calls, and, for many of the credit and fraud protection services, payment of money – while Defendant sits by and does nothing to assist those affected by the Data

Breach. Instead, as Defendant's Notice and website notification indicate, it is putting the burden on Plaintiffs and Class Members to discover possible fraudulent activity and identity theft.

104. Defendant's offer of twenty-four (24) months of credit monitoring and identity theft protection services to Plaintiffs and Class Members is woefully inadequate. While some harm has already begun, the worst may be yet to come. There may be a time lag between when harm occurs versus when it is discovered and also between when PII is acquired and when it is used. Furthermore, identity theft monitoring services only alert someone to the fact that they have already been the victim of identity theft (*i.e.*, fraudulent acquisition and use of another person's PII) – they do not prevent identity theft.[28]

CLASS ACTION ALLEGATIONS

105. Pursuant to Rule 23 of the Federal Rules of Civil Procedure, Plaintiffs bring this action on behalf of themselves and the following proposed Nationwide Class, defined as follows:

> **Nationwide Class**
>
> All persons residing in the United States who are current or former customers of T-Mobile or any T-Mobile affiliate, parent, or subsidiary, and had their PII compromised by an unknown third-party cybercriminal as a result of the Data Breach.

In addition, Plaintiffs bring this action on behalf of the following proposed Oklahoma Subclass defined as follows:

[28] *See, e.g.*, Kayleigh Kulp, *Credit Monitoring Services May Not Be Worth the Cost*, Nov. 30, 2017, https://www.cnbc.com/2017/11/29/credit-monitoring-services-may-not-be-worth-the-cost.html (last visited July 28, 2021).

Oklahoma Subclass

> All persons residing in the State of Oklahoma who are current or former customers of T-Mobile or any T-Mobile affiliate, parent, or subsidiary, and had their PII compromised as a result of the Data Breach.

106. Both the proposed Nationwide Class and the proposed Oklahoma Subclass will be collectively referred to as the Class, except where it is necessary to differentiate them.

107. Excluded from the proposed Class are any officer or director of Defendant; any officer or director of any affiliate, parent, or subsidiary of T-Mobile; anyone employed by counsel in this action; and any judge to whom this case is assigned, his or her spouse, and members of the judge's staff.

108. **Numerosity.** Members of the proposed Class likely number in the tens of thousands and are thus too numerous to practically join in a single action. Membership in the Class is readily ascertainable from Defendant's own records.

109. **Commonality and Predominance.** Common questions of law and fact exist as to all proposed Class Members and predominate over questions affecting only individual Class Members. These common questions include:

a. Whether Defendant engaged in the wrongful conduct alleged herein;

b. Whether Defendant's inadequate data security measures were a cause of the Data Breach;

c. Whether Defendant owed a legal duty to Plaintiffs and the other Class Members to exercise due care in collecting, storing, and safeguarding their

PII;

d. Whether Defendant negligently or recklessly breached legal duties owed to Plaintiffs and the Class Members to exercise due care in collecting, storing, and safeguarding their PII;

e. Whether Plaintiffs and the Class are at an increased risk for identity theft because of the Data Breach;

f. Whether Defendant failed to implement and maintain reasonable security procedures and practices for Plaintiffs' and Class Members' PII in violation Section 5 of the FTC Act;

g. Whether Plaintiffs and the other Class Members are entitled to actual, statutory, or other forms of damages, and other monetary relief; and

h. Whether Plaintiffs and the other Class Members are entitled to equitable relief, including, but not limited to, injunctive relief and restitution.

110. Defendant engaged in a common course of conduct giving rise to the legal rights sought to be enforced by Plaintiffs individually and on behalf of the other Class Members. Similar or identical statutory and common law violations, business practices, and injuries are involved. Individual questions, if any, pale by comparison, in both quantity and quality, to the numerous questions that dominate this action.

111. **Typicality:** Plaintiffs' claims are typical of the claims of the Members of the Class. All Class Members were subject to the Data Breach and had their PII accessed by and/or disclosed to unauthorized third parties. Defendant's misconduct affected all Class Members in the same manner.

112. **Adequacy of Representation:** Plaintiffs are adequate representatives of the Class because their interests do not conflict with the interests of the other Class Members they seek to represent; they have retained counsel competent and experienced in complex class action litigation, and Plaintiffs will prosecute this action vigorously. The interests of the Class will be fairly and adequately protected by Plaintiffs and their counsel.

113. **Superiority:** A class action is superior to any other available means for the fair and efficient adjudication of this controversy, and no unusual difficulties are likely to be encountered in the management of this matter as a class action. The damages, harm, or other financial detriment suffered individually by Plaintiffs and the other Class Members are relatively small compared to the burden and expense that would be required to litigate their claims on an individual basis against Defendant, making it impracticable for Class Members to individually seek redress for Defendant's wrongful conduct. Even if Class Members could afford individual litigation, the court system could not. Individualized litigation would create a potential for inconsistent or contradictory judgments and increase the delay and expense to all parties and the court system. By contrast, the class action device presents far fewer management difficulties and provides the benefits of single adjudication, economies of scale, and comprehensive supervision by a single court.

FIRST CAUSE OF ACTION
Negligence
(On behalf of Plaintiffs and the Nationwide Class or, alternatively, the Oklahoma Subclass)

114. Plaintiffs incorporate the foregoing paragraphs as though fully set forth herein.

115. Defendant owed a duty to Plaintiffs and the Class to exercise reasonable care in obtaining, securing, safeguarding, storing, and protecting Plaintiffs' and Class Members' PII from being compromised, lost, stolen, and accessed by unauthorized persons. This duty includes, among other things, designing, maintaining, and testing its data security systems to ensure that Plaintiffs' and Class Members' PII in Defendant's possession was adequately secured and protected.

116. Defendant owed a duty of care to Plaintiffs and Members of the Class to provide security, consistent with industry standards, to ensure that its protocols, systems, and networks adequately protected the PII of its current and former customers.

117. Defendant owed a duty of care to Plaintiffs and Class Members because they were foreseeable and probable victims of any inadequate data security practices. Defendant knew or should have known of the inherent risks in collecting and storing the PII of its current and former customers, especially in light of its recent history of data breaches; Defendant also should have known of the critical importance of adequately securing such information.

118. Plaintiffs and Class Members entrusted Defendant with their PII with the understanding that Defendant would safeguard it, that Defendant would not store it longer than necessary, and that Defendant was in a position to protect against the harm suffered by Plaintiffs and Class Members as a result of the Data Breach.

119. Defendant's own conduct also created a foreseeable risk of harm to Plaintiffs and Class Members and their PII. Defendant's misconduct included failing to implement the necessary systems, policies, employee training and procedures necessary to prevent the

Data Breach.

120. Defendant knew, or should have known, of the risks inherent in collecting and storing PII and the importance of adequate security. Defendant knew about – or should have been aware of – numerous, well-publicized data breaches affecting businesses in the United States.

121. Defendant breached its duties to Plaintiffs and Class Members by failing to provide fair, reasonable, or adequate computer systems and data security to safeguard the PII of Plaintiffs and Class Members.

122. Plaintiffs' injuries and damages, as described below, are a reasonably certain consequence of T-Mobile's breach of its duties.

123. Because Defendant knew that a breach of its systems would damage millions of current and former T-Mobile customers whose PII was being carelessly maintained, Defendant had a duty to improve its data systems and adequately protect the PII contained therein.

124. Defendant had a special relationship with current and former customers, including with Plaintiffs and Class Members, by virtue of their being current or former customers. Plaintiffs and Class Members reasonably believed that Defendant would take adequate security precautions to protect their PII. Defendant also had independent duties under state and federal laws that required Defendant to reasonably safeguard Plaintiffs' and Class Members' PII.

125. Through Defendant's acts and omissions, including Defendant's failure to provide adequate security and its failure to protect Plaintiffs' and Class Members' PII from

being foreseeably accessed, Defendant unlawfully breached its duty to use reasonable care to adequately protect and secure the PII of Plaintiffs and Class Members during the time it was within Defendant's possession or control.

126. By engaging in the negligent acts and omissions alleged herein, which permitted an unknown third party to access an T-Mobile's systems containing the PII at issue, Defendant failed to meet the data security standards set forth under Section 5 of the FTC Act, which prohibits "unfair…practices in or affecting commerce." This prohibition includes failing to have adequate data security measures, which Defendant has failed to do as discussed herein.

127. Defendant's failure to meet this standard of data security established under Section 5 of the FTC Act is evidence of negligence.

128. Neither Plaintiffs nor the other Class Members contributed to the Data Breach as described in this Complaint.

129. As a direct and proximate cause of Defendant's actions and inactions, including but not limited to its failure to properly encrypt its systems and otherwise implement and maintain reasonable security procedures and practices, Plaintiffs and Class Members have suffered and/or will suffer concrete injury and damages, including but not limited to: (i) the loss of the opportunity to determine for themselves how their PII is used; (ii) the publication and/or theft of their PII; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII, including the need for substantial credit monitoring and identity protection services for an extended period of time; (iv) lost opportunity costs associated with effort

expended and the loss of productivity addressing and attempting to mitigate the actual and 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; (v) costs associated with placing freezes on credit reports and password protection; (vi) anxiety, emotional distress, loss of privacy, and other economic and non-economic losses; (vii) the continued risk to their PII, 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 PII of customers and former 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 inevitable and continuing consequences of compromised PII for the rest of their lives.

SECOND CAUSE OF ACTION
Breach of Implied Contract
(On behalf of Plaintiffs and the Nationwide Class or, alternatively, the Oklahoma Subclass)

130. Plaintiffs incorporate the foregoing paragraphs as though fully set forth herein.

131. Defendant offered products and services to the current or former customers, including Plaintiffs and Class Members, in exchange for monetary payment.

132. As a condition of the purchase, Defendant required Plaintiffs and Class Members to provide their PII, including names, addresses, dates of birth, Social Security numbers, driver's license numbers, and other personal information. Implied in these exchanges was a promise by Defendant to ensure that the PII of Plaintiffs and Class

Members in its possession was only used to provide the agreed-upon products and services from Defendant.

133. These exchanges constituted an agreement between the parties: Plaintiffs and Class Members would provide their PII in exchange for the products and services provided by Defendant.

134. These agreements were made by Plaintiffs or Class Members who were customers of Defendant.

135. It is clear by these exchanges that the parties intended to enter into an agreement. Plaintiffs and Class Members would not have disclosed their PII to Defendant but for the prospect of Defendant's promise of providing the products and services purchased by Plaintiffs and the Class. Conversely, Defendant presumably would not have taken Plaintiffs' and Class Members' PII if it did not intend to provide Plaintiffs and Class Members with the bargained-for products and services.

136. Defendant was therefore required to reasonably safeguard and protect the PII of Plaintiffs and Class Members from unauthorized disclosure and/or use.

137. Plaintiffs and Class Members accepted Defendant's offer of products and services and fully performed their obligations under the implied contract with Defendant by providing payment and their PII, directly or indirectly, to Defendant, among other obligations.

138. Plaintiffs and Class Members would not have provided and entrusted their PII to Defendant in the absence of their implied contracts with Defendant and would have instead retained the opportunity to control their PII for uses other than the purchase and

use of T-Mobile products and services.

139. Defendant breached the implied contracts with Plaintiffs and Class Members by failing to reasonably safeguard and protect Plaintiffs' and Class Members' PII.

140. Defendant's failure to implement adequate measures to protect the PII of Plaintiffs and Class Members violated the purpose of the agreement between the parties.

141. Defendant was on notice that its systems and data security protocols were inadequate yet failed to invest in the proper safeguarding of Plaintiffs' and Class Members' PII.

142. Instead of spending adequate financial resources to safeguard Plaintiffs' and Class Members' PII, which Plaintiffs and Class Members were required to provide to Defendant, Defendant instead used that money for other purposes, thereby breaching its implied contracts it had with Plaintiffs and Class Members.

143. As a proximate and direct result of Defendant's breaches of its implied contracts with Plaintiffs and Class Members, Plaintiffs and the Class Members suffered damages as described in detail above.

THIRD CAUSE OF ACTION
Breach of Confidence
(On behalf of Plaintiffs and the Nationwide Class or, alternatively, the Oklahoma Subclass)

144. Plaintiffs incorporate the foregoing paragraphs as though fully set forth herein.

145. At all times during Plaintiffs' and Class Members' interactions with Defendant as its customers, Defendant was fully aware of the confidential and sensitive

nature of Plaintiffs' and Class Members' PII that Plaintiffs and Class Members provided to Defendant.

146. Plaintiffs' and Class Members' PII constitutes confidential and novel information. Indeed, Plaintiffs' and Class Members' Social Security numbers can be changed only with great difficulty and time spent, which still enables a threat actor to exploit that information during the interim; additionally, 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.

147. As alleged herein and above, Defendant's relationship with Plaintiffs and Class Members was governed by terms and expectations that Plaintiffs' and Class Members' PII would be collected, stored, and protected in confidence, and would not be disclosed to unauthorized third parties.

148. Plaintiffs and Class Members provided their respective PII to Defendant with the explicit and implicit understandings that Defendant would protect and not permit the PII to be disseminated to any unauthorized parties.

149. Defendant voluntarily received in confidence Plaintiffs' and Class Members' PII with the understanding that the PII would not be disclosed or disseminated to the public or any unauthorized third parties.

150. Due to Defendant's failure to prevent, detect, and avoid the Data Breach from occurring by, *inter alia*, not following best information security practices and by not

providing proper employee training to secure Plaintiff's and Class Members' PII, Plaintiffs' and Class Members' PII was disclosed and misappropriated to unauthorized third parties beyond Plaintiffs' and Class Members' confidence, and without their express permission.

151. As a direct and proximate cause of Defendant's actions and/or omissions, Plaintiffs and Class Members have suffered damages.

152. But for Defendant's disclosure of Plaintiffs' and Class Members' PII, in violation of the parties' understanding of confidence, Plaintiffs' and Class Members' PII would not have been compromised, stolen, viewed, accessed, and used by unauthorized third parties. Defendant's Data Breach was the direct and legal cause of the theft of Plaintiffs' and Class Members' PII, as well as the resulting damages.

153. This disclosure of Plaintiffs' and Class Members' PII constituted a violation of Plaintiffs' and Class Members' understanding that Defendant would safeguard and protect the confidential and novel PII that Plaintiffs and Class Members were required to disclose to Defendant.

154. The concrete injury and harm Plaintiffs and Class Members suffered was the reasonably foreseeable result of Defendant's unauthorized disclosure of Plaintiffs' and Class Members' PII. Defendant knew its data security procedures for accepting and securing Plaintiffs' and Class Members' PII had numerous security and other vulnerabilities that placed Plaintiffs' and Class Members' PII in jeopardy.

155. As a direct and proximate result of Defendant's breaches of confidence, Plaintiffs and Class Members have suffered and/or are at a substantial risk of suffering

concrete injury that includes but is not limited to: (a) actual identity theft; (b) the compromise, publication, and/or theft of their PII; (c) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft and/or unauthorized use of their PII; (d) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (e) the continued risk to their PII, 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 PII in its continued possession; and (f) future costs in terms of time, effort, and money that will be expended as result of the Data Breach for the remainder of the lives of Plaintiffs and Class Members.

FOURTH CAUSE OF ACTION
Invasion of Privacy
(On behalf of Plaintiffs and the Nationwide Class or, alternatively, the Oklahoma Subclass)

156. Plaintiffs incorporate the foregoing paragraphs as though fully set forth herein.

157. Oklahoma establishes the right to privacy in the Oklahoma Constitution's Right to Privacy clause. *See* Okla. Const. Art. II, Section 30.

158. Plaintiffs and Class Members had a legitimate and reasonable expectation of privacy with respect to their PII and were accordingly entitled to the protection of this personal information against disclosure to and acquisition by unauthorized third parties.

159. Defendant owed a duty to its customers, including Plaintiffs and Class Members, to keep their PII private and confidential.

160. The unauthorized access, acquisition, appropriation, disclosure, encumbrance, exfiltration, release, theft, use, and/or viewing of PII, especially the PII that is the subject of this action, is highly offensive to a reasonable person.

161. This intrusion of privacy was an intrusion into a place or thing belonging to Plaintiffs and Class Members that was private and is entitled to remain private. Plaintiffs and Class Members disclosed their PII to Defendant as part of their purchases of Defendant's products and services, but did so privately with the intention and understanding that the PII would be kept confidential and protected from unauthorized access, acquisition, appropriation, disclosure, encumbrance, exfiltration, release, theft, use, and/or viewing. Plaintiffs and Class Members were reasonable in their belief that such information would be kept private and would not be disclosed without their authorization. The Data Breach, which was caused by Defendant's negligent actions and inactions, constitutes an intentional interference with Plaintiffs' and Class Members' interest in solitude or seclusion, either as to their persons or as to their private affairs or concerns, of a kind that would be highly offensive to a reasonable person.

162. Defendant acted with a knowing state of mind when it permitted the Data Breach because it knew its information security practices were inadequate.

163. Defendant invaded Plaintiff's and Class Members' privacy by failing to adequately implement data security measures, despite its obligations to protect current and former customers' highly sensitive PII.

164. Defendant's motives leading to the Data Breach were financially based. In order to save on operating costs, Defendant decided against the implement of adequate data security measures.

165. Defendant's intrusion upon Plaintiffs' and Class Members' privacy in order to save money constitutes an egregious breach of social norms.

166. Acting with knowledge, Defendant had notice and knew that its inadequate cybersecurity practices would cause injury to Plaintiffs and Class Members.

167. As a proximate result of Defendant's acts and omissions, Plaintiffs' and Class Members' PII was accessed by, acquired by, appropriated by, disclosed to, encumbered by, exfiltrated by, obtained by, released to, stolen by, used by, and/or viewed by third parties without authorization, causing Plaintiffs and Class Members to suffer concrete damages as described herein.

168. Unless and until enjoined and restrained by order of this Court, Defendant's wrongful conduct will continue to cause great and irreparable injury to Plaintiffs and Class Members in that the PII maintained by Defendant can still be accessed by, acquired by, appropriated by, disclosed to, encumbered by, exfiltrated by, released to, stolen by, used by, and/or viewed by unauthorized persons.

169. Plaintiffs and Class Members have no adequate remedy at law for the injuries they have suffered and are at imminent risk of suffering in that a judgment for monetary damages will not end the invasion of privacy for Plaintiffs and Class Members.

FIFTH CAUSE OF ACTION
Breach of Fiduciary Duty
(On behalf of Plaintiffs and the Nationwide Class or, alternatively, the Oklahoma

Subclass)

170. Plaintiffs incorporate the foregoing paragraphs as though fully set forth herein.

171. In light of their special relationship, Defendant became the guardian of Plaintiffs' and Class Members' PII. Defendant became a fiduciary, created by its undertaking and guardianship of its customers' PII, to act primarily for the benefit of those customers, including Plaintiffs and Class Members. This duty included the obligation to safeguard Plaintiffs' and Class Members' PII and to timely detect and notify them in the event of a data breach.

172. In order to provide Plaintiffs and Class Members compensation and employment benefits, or to even consider Plaintiffs and Class Members for employment, Defendant required that Plaintiffs and Class Members provide their PII.

173. Defendant knowingly undertook the responsibility and duties related to the possession of Plaintiffs' and Class Members' PII for the benefit of Plaintiffs and Class Members in order to provide Plaintiffs and Class Members compensation and employment benefits.

174. Defendant has a fiduciary duty to act for the benefit of Plaintiffs and Class Members upon matters within the scope of its relationship with them. Defendant breached its fiduciary duties owed to Plaintiffs and Class Members by failing to properly encrypt and otherwise protect Plaintiffs' and Class Members' PII. Defendant further breached its fiduciary duties owed to Plaintiffs and Class Members by failing to timely detect the Data Breach and notify and/or warn Plaintiffs and Class Members of the Data Breach.

175. As a direct and proximate result of Defendant's breaches of its fiduciary duties, Plaintiffs and Class Members have suffered or will suffer concrete injury, including but not limited to (a) actual identity theft; (b) the loss of the opportunity of how their PII is used; (c) the unauthorized access, acquisition, appropriation, disclosure, encumbrance, exfiltration, release, theft, use, and/or viewing of their PII; (d) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft and/or unauthorized use of their PII; (e) lost opportunity costs associated with efforts expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (f) the continued risk to their PII, 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 Plaintiff's and Class Members' PII in its continued possession; and (g) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PII compromised as a direct and traceable result of the Data Breach for the remainder of the lives of Plaintiffs and Class Members.

176. As a direct and proximate result of Defendant's breach of its fiduciary duty, Plaintiffs and Class Members have suffered and will continue to suffer other forms of injury and/or harm, and other economic and non-economic losses.

SIXTH CAUSE OF ACTION
Breach of Covenant of Good Faith and Fair Dealing
(On behalf of Plaintiffs and the Nationwide Class or, alternatively, the Oklahoma Subclass)

177. Plaintiffs incorporate the foregoing paragraphs as though fully set forth herein.

178. As described above, when Plaintiffs and the Class Members provided their PII to Defendant, they entered into implied contracts in which Defendant agreed to comply with its statutory and common law duties and industry standards to protect Plaintiffs' and Class Members' PII and to timely detect and notify them in the event of a data breach.

179. These exchanges constituted an agreement between the parties: Plaintiffs and Class Members were required to provide their PII in exchange for products and services provided by Defendant, as well as an implied covenant by Defendant to protect Plaintiffs' PII in its possession.

180. It was clear by these exchanges that the parties intended to enter into an agreement. Plaintiffs and Class Members would not have disclosed their PII to Defendant but for the prospect of Defendant's promise of certain products and services. Conversely, Defendant presumably would not have taken Plaintiffs' and Class Members' PII if it did not intend to provide Plaintiffs and Class Members with the products and services it was offering.

181. Implied in these exchanges was a promise by Defendant to ensure that the PII of Plaintiffs and Class Members in its possession was only used to provide the agreed-upon products and services.

182. Plaintiffs and Class Members therefore did not receive the benefit of the bargain with Defendant, because they provided their PII in exchange for T-Mobile's implied agreement to keep it safe and secure.

183. While Defendant had discretion in the specifics of how it met the applicable laws and industry standards, this discretion was governed by an implied covenant of good faith and fair dealing.

184. Defendant breached this implied covenant when it engaged in acts and/or omissions that are declared unfair trade practices by the FTC and state statutes and regulations. These acts and omissions included: omitting, suppressing, and concealing the material fact of the inadequacy of the privacy and security protections for Plaintiffs' and Class Members' PII; storing the PII of former customers, despite any valid purpose for the storage thereof having ceased upon the termination of the business relationship with those individuals; and failing to disclose to Plaintiffs and Class Members at the time they provided their PII to it that Defendant's data security systems failed to meet applicable legal and industry standards.

185. Plaintiffs and Class Members did all or substantially all the significant things that the contract required them to do.

186. Likewise, all conditions required for Defendant's performance were met.

187. Defendant's acts and omissions unfairly interfered with Plaintiffs' and Class Members' rights to receive the full benefit of their contracts.

188. Plaintiffs and Class Members have been or will be harmed by Defendant's breach of this implied covenant in the many ways described above, including actual identity theft and/or imminent risk of certainly impending and devastating identity theft that exists now that cyber criminals have their PII, and the attendant long-term expense of attempting to mitigate and insure against these risks.

189. Defendant is liable for its breach of these implied covenants, whether or not it is found to have breached any specific express contractual term.

190. Plaintiffs and Class Members are entitled to damages, including compensatory damages and restitution, declaratory and injunctive relief, and attorney fees, costs, and expenses.

SEVENTH CAUSE OF ACTION
Declaratory and Injunctive Relief
(On behalf of Plaintiffs and Nationwide Class or, alternatively, the Oklahoma Subclass)

191. Plaintiffs incorporate the foregoing paragraphs as though fully set forth herein.

192. This Count is brought under the federal Declaratory Judgment Act, 28 U.S.C. §2201.

193. As previously alleged, Plaintiffs and Class Members entered into an implied contract that required Defendant to provide adequate security for the PII it collected from Plaintiffs and Class Members.

194. Defendant owes a duty of care to Plaintiffs and Class Members requiring it to adequately secure their PII.

195. Defendant still possesses Plaintiffs' and Class Members' PII.

196. Since the Data Breach, Defendant has announced few, if any, changes to its data security infrastructure, processes, or procedures to fix the vulnerabilities in its computer systems and/or security practices which permitted the Data Breach to occur and, thereby, prevent future attacks.

197. Defendant has not satisfied its contractual obligations and legal duties to Plaintiffs and Class Members. In fact, now that Defendant's insufficient data security is known to hackers, the PII in Defendant's possession is even more vulnerable to cyberattack.

198. Actual harm has arisen in the wake of the Data Breach regarding Defendant's contractual obligations and duties of care to provide security measures to Plaintiffs and Class Members. Further, Plaintiffs and Class Members are at risk of additional or further harm due to the exposure of their PII and Defendant's failure to address the security failings that led to such exposure.

199. There is no reason to believe that Defendant's security measures are any more adequate now than they were before the Data Breach to meet Defendant's contractual obligations and legal duties.

200. Plaintiffs, therefore, seek a declaration (1) that Defendant's existing security measures do not comply with its contractual obligations and duties of care to provide adequate security, and (2) that to comply with its contractual obligations and duties of care, Defendant must implement and maintain reasonable security measures, including, but not limited to:

a. Ordering that Defendant engage 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

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

b. Ordering that Defendant engage third-party security auditors and internal personnel to run automated security monitoring;

c. Ordering that Defendant audit, test, and train its security personnel regarding any new or modified procedures;

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

e. Ordering that Defendant purge, delete, and destroy in a reasonably secure manner customer data not necessary for its provisions of services;

f. Ordering that Defendant conduct regular computer system scanning and security checks;

g. Ordering that Defendant routinely and continually conduct internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach; and

h. Ordering Defendant to meaningfully educate its current, former, and prospective customers about the threats they face as a result of the loss of their PII to third parties, as well as the steps they must take to

protect themselves.

EIGHTH CAUSE OF ACTION
VIOLATIONS OF OKLAHOMA CONSUMER PROTECTION ACT, OKLA. STAT., TIT. 15, CH. 20 §§751, *et seq*
(On Behalf of Plaintiffs and the Class)

201. Plaintiffs incorporate the foregoing paragraphs as though fully set forth herein.

202. The Oklahoma Consumer Protection Act ("OCPA"), Okla. Stat. tit. 15, §§751, *et seq*., prohibits unfair unfair or deceptive trade practices in the course of a person's business. *See* Okla. Stat. tit. 15, §§752(13)-(14), 753(20).

203. T-Mobile is a "person," as meant by Okla. Stat. tit. 15, §752(1).

204. Plaintiffs and members of the Class are "aggrieved consumers" within the meaning of the OCPA.

205. T-Mobile offers, sells, and distributes goods, services, and other things of value, which constitute "consumer transactions" as meant by Okla. Stat. tit. 15, §752(2).

206. T-Mobile, in the course of its business, engaged in unlawful practices in violation of Okla. Stat. tit. 15, §753, including the following:

a. making false representations, knowingly or with reason to know, as to the characteristics, uses, and benefits of the subjects of its consumer transactions, in violation of Okla. Stat. tit. 15, §753(5);

b. representing, knowingly or with reason to know, that the subjects of its consumer transactions were of a particular standard when they were of another, in violation of Okla. Stat. tit 15, §753(7);

c. advertising, knowingly or with reason to know, the subjects of its consumer transactions with intent not to sell as advertised, in violation of Okla. Stat. tit 15, §753 (8);

d. committing unfair trade practices that offend established public policy and was immoral, unethical, oppressive, unscrupulous, and substantially injurious to consumers as defined by section 752(14), in violation of Okla. Stat. tit. 15, §753(20); and

e. committing deceptive trade practices that deceived or could reasonably be expected to deceive or mislead a person to the detriment of that person as defined by section 752(13), in violation of Okla. Stat. tit. 15, §753(20).

207. T-Mobile's unlawful practices include:

a. Unreasonably adopting and maintaining data security measures that were inadequate to protect Plaintiffs' and Class Members' PII, which was a direct and proximate cause of the Data Breach;

b. Ignoring actual and foreseeable security and privacy risks that lead to the Data Breach;

c. Implementing inadequate security and privacy measures, which was a direct and proximate cause of the Data Breach;

d. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Class Members' PII, including duties imposed by the FTC Act;

e. omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiffs' and Class Members' PII; and

f. omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Class Members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. §45.

208. T-Mobile's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of T-Mobile's data security and ability to protect the confidentiality of consumers' PII.

209. Had T-Mobile disclosed to Plaintiffs and Class Members that its data systems were not secure and, thus, vulnerable to attack, T-Mobile would have been unable to continue in business and it would have been forced to adopt reasonable data-security measures and comply with the law.

210. Instead, T-Mobile held itself out as having adequate data security practices to keep Plaintiffs' and Class Members' PII safe from intrusion and exfiltration by unauthorized third parties.

211. These unlawful practices and acts by T-Mobile were immoral, unethical, oppressive, unscrupulous, and substantially injurious. These acts caused substantial injury to Plaintiffs and Class Members.

212. Further, the injuries suffered by Plaintiffs and the Class are not outweighed by any countervailing benefits to consumers or competition. And, because T-Mobile is

solely responsible for securing its networks and protecting PII, there is no way Plaintiffs or the Class could have known about T-Mobile's inadequate data security practices or avoided the injuries they sustained from the Data Breach. There were reasonably available alternatives to further T-Mobile's legitimate business interests, other than its conduct responsible for the Data Breach.

213. T-Mobile's conduct is also unconscionable within the meaning of OCPA because it undermines public policy that businesses protect personal and financial information, as reflected in the FTC Act.

214. T-Mobile acted intentionally, knowingly, and maliciously to violate OCPA, and recklessly disregarded Plaintiffs' and the Class Members' rights.

215. As a direct and proximate result of T-Mobile's unlawful practices, Plaintiffs and Class Members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their PII.

216. Plaintiffs and Class Members seek all monetary and non-monetary relief allowed by law, including actual damages, civil penalties, and attorneys' fees and costs.

NINTH CAUSE OF ACTION
Violation of the Oklahoma Deceptive Trade Practices Act, 78 O.S. §§51, et seq.
(On Behalf of Plaintiff and the Class)

217. Plaintiffs incorporate the foregoing paragraphs as though fully set forth herein.

218. The Oklahoma Deceptive Trade Practices Act ("Oklahoma DTPA"), 78 O.S.

§§51, et seq., prohibits deceptive trade practices in the course of a person's business, vocation, or occupation. 78 O.S. §53(A).

219. T-Mobile is a "person," as meant by 78 O.S. §52(8).

220. Plaintiffs and members of the Class are "persons" under 78 O.S. §52(8). Plaintiffs and the Class are consumers whose PII was in T-Mobile's possession.

221. T-Mobile, in the course of its business, engaged in deceptive practices in violation of 78 O.S. §§53(A), including the following:

a. Knowingly making false representations as to the characteristics, uses, and benefits of its goods and services, in violation of 78 O.S.§§53(A)(5); and

b. Knowingly representing that its goods and services are of a particular standard when they were of another, in violation of 78 O.S.§§53(A)(7).

222. T-Mobile's deceptive practices include:

a. Unreasonably adopting and maintaining data security measures that were inadequate to protect PII, which was a direct and proximate cause of the Data Breach;

b. Ignoring foreseeable security risks, refusing to remediate identified security risks, and failing to adequately improve security measures following previous cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law to avoid causing foreseeable risk of harm and statutory duties pertaining to the security of PII, including duties imposed by the FTC Act, which was a direct and proximate cause of the Data Breach;

d. Misrepresenting that it would protect PII, including by implementing and maintaining reasonable security measures; and

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security of PII, including duties imposed by the FTC Act.

223. T-Mobile's conduct caused substantial injury to consumers and provided no benefit to consumers or competition. The injuries suffered by Plaintiffs and the Class are not outweighed by any countervailing benefits to consumers or competition. And, because T-Mobile is solely responsible for securing its networks and protecting PII, there is no way Plaintiffs or Class Members could have known about T-Mobile's inadequate data security practices or avoided the injuries they sustained. There were reasonably available alternatives to further T-Mobile's legitimate business interests, other than its conduct responsible for the Data Breach.

224. T-Mobile intended to mislead Plaintiff and Class and induce them to rely on its misrepresentations.

225. Had T-Mobile disclosed to Plaintiffs and Class that its data systems were not secure and, thus, vulnerable to attack, T-Mobile would have been unable to continue in business and it would have been forced to adopt reasonable data security measures and

comply with the law.

226. Instead, T-Mobile held itself out as having adequate data security practices to keep Plaintiffs' and Class Members' PII safe from intrusion and exfiltration by unauthorized third parties.

227. Accordingly, T-Mobile's representations were material because they were likely to deceive reasonable financial institutions about the adequacy of T-Mobile's data security and ability to protect the confidentiality of PII, and Plaintiffs and the Class acted reasonably in relying on T-Mobile's misrepresentations, the truth of which they could not have discovered.

228. As a direct and proximate result of T-Mobile's unlawful practices, Plaintiffs and the Class have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring accounts for fraudulent activity; and an increased, imminent risk of fraud and identity theft.

229. Plaintiffs and the Class seek all monetary and non-monetary relief allowed by law, including actual damages, civil penalties, and attorneys' fees and costs.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, individually, and on behalf of themselves and all others similarly situated, and on behalf of the general public, respectfully request that the Court enter an order:

a. Certifying the proposed Class as requested herein;

b. Appointing Plaintiffs as Class Representatives and the undersigned counsel

as Class Counsel;

c. Finding that Defendant engaged in the unlawful conduct as alleged herein;

d. Granting 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:

i. prohibiting T-Mobile from engaging in the wrongful and unlawful acts described herein;

ii. requiring T-Mobile 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;

iii. requiring T-Mobile to delete, destroy, and purge the PII of Plaintiffs and Class Members unless T-Mobile 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;

iv. requiring T-Mobile to implement and maintain a comprehensive information security program designed to protect the confidentiality and integrity of the PII of Plaintiffs and Class Members' PII;

v. prohibiting T-Mobile from maintaining Plaintiffs' and Class Members' PII on a cloud-based database;

vi. requiring T-Mobile 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 T-Mobile's systems on a periodic basis, and ordering T-Mobile to promptly correct any problems or issues detected by such third-party security auditors;

vii. requiring T-Mobile to engage independent third-party security auditors and internal personnel to run automated security monitoring;

viii. requiring T-Mobile to audit, test, and train its security personnel regarding any new or modified procedures;

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

x. requiring T-Mobile to conduct regular database scanning and securing checks;

xi. requiring T-Mobile 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 PII, as well as protecting the PII of Plaintiffs and Class Members;

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

xiii. requiring T-Mobile 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 T-Mobile's policies, programs, and systems for protecting PII;

xiv. requiring T-Mobile to implement, maintain, regularly review, and revise as necessary a threat management program designed to appropriately monitor T-Mobile's information networks for threats, both internal and external, and assess whether monitoring tools are appropriately configured, tested, and updated;

xv. requiring T-Mobile to meaningfully educate all Class Members about the threats that they face as a result of the loss of their confidential PII to third parties, as well as the steps affected individuals must take to protect themselves;

xvi. requiring T-Mobile to implement logging and monitoring programs sufficient to track traffic to and from T-Mobile's servers;

xvii. 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 T-Mobile'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;

xviii. requiring Defendant to design, maintain, and test its computer systems to ensure that PII in its possession is adequately secured and protected;

xix. requiring Defendant to implement multi-factor authentication requirements, if not already implemented;

xx. requiring Defendant's employees to change their passwords on a timely and regular basis, consistent with best practices; and

xxi. requiring Defendant to provide lifetime credit monitoring and identity theft repair services to Class Members.

e. Awarding Plaintiffs and Class Members damages;

f. Awarding Plaintiffs and Class Members pre-judgment and post-judgment interest on all amounts awarded;

g. Awarding Plaintiffs and the Class Members reasonable attorneys' fees, costs, and expenses; and

h. Granting such other relief as the Court deems just and proper.

DEMAND FOR JURY TRIAL

Plaintiffs, on behalf of themselves and the proposed Class, as well as on behalf of

the general public, hereby demand a trial by jury as to all matters so triable.

Date: August 23, 2021

Respectfully Submitted,

s/ William B. Federman
William B. Federman, OBA #2853
Tyler J. Bean, OBA #33834
Molly E. Brantley, OBA #33126
FEDERMAN & SHERWOOD
10205 N. Pennsylvania Ave.
Oklahoma City, OK 73120
Telephone: (405) 235-1560
Facsimile: (405) 239-2112
wbf@federmanlaw.com
tjb@federmanlaw.com
meb@federmanlaw.com

Cornelius Dukelow, OBA #19086
ABINGTON COLE + ELLERY
320 South Boston Avenue
Suite 1130
Tulsa, Oklahoma 74103
Telephone: (918) 588-3400
cdukelow@abingtonlaw.com

Attorneys for Plaintiffs and the Class