UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF TEXAS

ANNA TRUSS, on behalf of herself and all others similarly situated, Plaintiff v. DELL INC. Defendant	Civil Action No.: 1:24-cv-00647 **CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

Plaintiff Anna Truss ("Truss" or "Plaintiff"), by and through her attorneys of record, upon personal knowledge as to her own acts and experiences, and upon information and belief as to all other matters, which Plaintiff believes will be supplemented and supported after a reasonable opportunity for discovery, brings this class action complaint against defendant Dell Inc. ("Dell" or "Defendant"), and alleges as follows:

INTRODUCTION

1. Plaintiff brings this class action against Defendant for its failure to properly secure and safeguard Plaintiff's and Class Members' protected "personally identifiable information" or "PII" (also referred to herein as "Private Information").[1]

[1] Personally identifiable information ("PII") 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 C.F.R. § 200.79. At a minimum, the term "PII" or "Private information" as used herein, includes all information that, on its face, expressly identifies an individual. PII or Private Information 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 numbers, and financial information).

2. Dell, based in Austin, Texas, is a one of the largest computer manufacturers in the world, manufacturing and marketing desktop and laptop computers, monitors and other computer accessories and services throughout the United States.

3. In the course of providing its services, Defendant acquired and collected Plaintiff's and Class Members' PII. Defendant knew at all times material that it was collecting, and responsible for the security of sensitive data, including Plaintiff's and Class Members' highly confidential PII. This PII remains in the possession of Defendant, despite the fact that it was accessed by unauthorized third persons, is currently being maintained without appropriate and necessary safeguards, independent review, and oversight, and therefore remains vulnerable to additional hackers and theft.

4. Plaintiff seeks to hold Defendant responsible for the harms it caused and will continue to cause Plaintiff and approximately 49 million other similarly situated persons by virtue of a preventable third party cyberattack that Dell detected at an undisclosed point prior to May 9, 2024. As a consequence of this cyberattack, Private Information -PII- that Defendant was entrusted with and responsible for, was accessed and exfiltrated (the "Data Breach"). This Private Information is significantly valuable to data thieves. Plaintiff further seeks to hold Defendant responsible for not ensuring that the PII was maintained in a manner consistent with industry standards.

5. The Data Breach was a direct result of Defendant's failure to implement adequate and reasonable cyber-security procedures and protocols necessary to protect Plaintiff's and Class Members' PII. The Data Breach occurred because Defendant maintained Class Members' PII in a reckless manner, and on its computer networks in a condition that was vulnerable to cyber-attack.

6. The risk of cyber-attack was well-known to Defendant and it was continuously on notice at all times material that its failure to take steps necessary to secure the PII from a risk of cyber-attack and unauthorized access left that information and property in a dangerous condition that was vulnerable to theft and misuse.

7. Defendant has not disclosed when it learned of the Data Breach. However, Defendant failed to disclose the event, or otherwise provide its individual clients notice of the Data Breach, until May 9, 2024. Defendant further prejudiced Plaintiff and Class Members by understating the significance of the data breach and failing to disclose the full extent of the data accessed in the Data Breach. Defendant's failure to adequately inform Plaintiff and Class Members of the extent of, and risks posed by, the Data Breach was highly prejudicial to Plaintiff and Class Members.

8. By obtaining, collecting, using, and deriving a benefit from Plaintiff's and Class Members' PII, Defendant assumed legal and equitable duties to those individuals. These duties arise from state and federal statutes and regulations, as well as common law principles.

9. Defendant disregarded the rights of Plaintiff and Class Members by intentionally, willfully, recklessly, or negligently failing to take and implement adequate and reasonable measures to ensure that Plaintiff's and Class Members' PII was safeguarded, failing to take available steps to prevent an unauthorized disclosure of data, and failing to follow applicable, required, and appropriate protocols, policies, and procedures regarding the encryption of data, even for internal use. As a result, upon information and belief, the PII of Plaintiff and Class Members was compromised and damaged through access by and disclosure to an unknown and unauthorized third party—an undoubtedly nefarious third party that seeks to profit off this disclosure by defrauding Plaintiff and Class Members in the future – thus entitling them to damages. In addition, Plaintiff and Class Members, who have a continuing interest in ensuring that their information is and remains safe, are entitled to injunctive and other equitable relief.

PARTIES

Plaintiff Anna Truss

10. Plaintiff Truss is, and at all relevant times was, a citizen of the state of Washington and a resident of Lynnwood, Snohomish County. Plaintiff Truss purchased a personal computer from Dell on November 26, 2023. In order to complete this purchase, Plaintiff Truss provided

substantial Personal Information to Defendant, including, but not limited to, her full name, contact information, and payment information. In addition, in connection with her application for credit offered by Dell, referred to as "Dell Pay," Plaintiff Truss, provided her Social Security Number, birthdate, and financial account information.

11. On May 24, 2024, Plaintiff Truss received emails and a telephone call from an individual or individuals purporting to be Dell employees. These email communications included substantial details regarding Plaintiff Truss' purchase of her Dell computer including the date of the purchase, the total amount paid, and the methods of payment used by Plaintiff Truss, for the purchase of her Dell computer. A May 24, 2024 email, purportedly from a dell.com email address, purported to inform Plaintiff Truss of an "issue with your payment method[,]" stating that "there was an issue with your payment method and the payment could not be processed." This email identified the relevant purchase date, the total amount of the purchase and identified a balance due of $325.87, the amount that Plaintiff Truss had paid using Dell's branded credit, "Dell Pay."

12. In a second email, also received on May 24, 2024, purportedly from the same Dell.com email address, the sender asserted that "I see that you have paid $600 for this invoice" and identified the credit card issuer used by Plaintiff Truss for the purchase of her Dell computer and further stated that "however, remaining payment of $325.87 was not captured due to a payment decline by your Comenity Capital bank (Dell Pay)." Significantly, this email identified the payment methods used by Plaintiff Truss and the amounts of the payments remitted through those respective payment methods. This email continued by offering to provide one of several alternative payment options for the purported remaining balance, including a PayPal link, a contact via phone so "you can give me the credit card details so our internal team will securely charge" the outstanding payment, or a link to the "Dell Pay Now" platform.

13. In addition to these emails, Plaintiff Truss received a telephone call, again purportedly from a Dell employee, seeking payment.

14. Plaintiff Truss takes care in protecting her PII from disclosure. Faced with the risk of the unauthorized disclosure of her PII, she is now forced to monitor her financial accounts for

signs of fraud and identity theft and devote valuable time and resources to same. Plaintiff has taken affirmative steps to freeze her credit.

Defendant Dell Inc.

15. Defendant is a computer technology corporation headquartered at One Dell Way, Round Rock Texas. Describing itself as "creat[ing] the technologies that drive human progress[,]" Dell manufactures and markets desktop and laptop computers and computer peripherals throughout the United States.[2] Dell is a wholly-owned subsidiary of Dell Technologies, Inc.

16. In the course of selling goods to consumers, Defendant collects and requires its customers to provide PII.

17. By obtaining, collecting, using, and deriving benefit from Plaintiff's and Class Members' PII, Defendant assumed legal and equitable duties to those persons and knew, or should have known, that it was responsible for protecting Plaintiff's and Class Members' PII from unauthorized disclosure and/or criminal hacking activity.

JURISDICTION AND VENUE

18. This Court has original jurisdiction over this action pursuant to 28 U.S.C. § 1332(d)(2), because the matter in controversy, exclusive of interest and costs, exceeds the sum value of $5,000,000.00, consists of putative class membership of greater than 100 members, and is a class action in which some of the members of the Class are citizens of states different than that of Defendant.

19. Venue is proper in this Court pursuant to 28 U.S.C. § 1391 because Defendant is authorized to conduct business within this District, is headquartered in this District, has intentionally availed itself of the laws in this District, and conducts substantial business, including acts underlying the allegations of this complaint, in this District.

[2] https://www.dell.com/en-us/dt/corporate/about-us/who-we-are.htm, last visited on May 31, 2024.

FACTUAL BACKGROUND

Dell's Business Involving the Collection and Maintenance of Private Information

20. Founded in 1984, Dell directly markets computers and peripherals to consumers. Since its founding, Dell has grown to be one of the largest computer manufacturers in the world.

21. Defendant requires those persons and entities that purchase its computers and other peripherals to provide their Private Information, which Defendant is obligated to keep confidential and private.

22. In its "Privacy Statement Regarding Customer and Online User Information" ("Privacy Statement") Dell acknowledges the collection of PII, including: "your email address, name, home address and telephone number. If you make a purchase, we may ask for your credit card number and billing information. We may also ask for your Social Security number and other data to process your credit or financing request."[3] Dell assures consumers that it

23. Defendant's Privacy Policy expressly comforts clients and their patients with the representation that it "***takes all reasonable steps*** to protect your Personal Information from misuse, interference and loss, as well as unauthorized access, modification or disclosure."[4] (Emphasis added).

The Data Breach

24. On May 9, 2024, Defendant issued a notice (the "Notice") via email stating that it was "currently investigating an incident involving a Dell portal, which contains a database with limited types of customer information related to purchases from Dell."[5] In the Notice, Dell assured impacted customers both that "[w]e believe there is not a significant risk to our customers given the type of information involved" and that "[t]he information involved does not include financial

---

[3] https://www.dell.com/learn/ai/en/aicorp1/policies-privacy?s=corp (last visited May 31, 2024).

[4] *Id.*

[5] A copy of the Notice Received by Plaintiff Truss is filed herewith as Exhibit A.

or payment information, email address, telephone number or any highly sensitive customer information."[6] Finally, Dell assured recipients of its Notice that "we do not believe there is significant risk given the limited information impacted."[7]

25. Despite these assertions, as set forth above, it appears that the Data Breach was substantially broader, including financial and/or payment information, and significant transaction details, giving rise to significant exposure to financial fraud and phishing attacks by which hackers can gain additional information from Class Members, further exposing them to the financial fraud and identity theft. Moreover, because consumers utilizing Dell's Dell Pay credit offering are required to provide, *inter alia*, Social Security numbers and other critical PII, it is unclear whether Plaintiff and Class Members are at continued risk of identity theft.

26. The Data Breach enabled unauthorized cybercriminals to access very private and sensitive PII.

Dell's Business and Obligation to Preserve and Protect Confidentiality and Privacy

27. As acknowledge in its Privacy Policy, Defendant is entrusted with highly sensitive PII, including names, contact information, Social Security Numbers, and other highly sensitive PII. Defendant retains and stores this information and derives a substantial economic benefit from the PII that it collects.

28. Plaintiff and Class Members are current or former customers of Defendant.

29. Plaintiff and Class Members provided their PII with the reasonable expectation and mutual understanding that Defendant would comply with its obligations to keep such information confidential and secure from unauthorized access, and Defendant expressly represented in its Privacy Policy that it would do so.

30. Plaintiff and Class Members relied on Defendant to keep their Private Information confidential and securely maintained, to use this information for necessary purposes only, and to

6 Ex. A.

7 Id.

make only authorized disclosures of this information. Plaintiff and Class Members, who value the confidentiality of their Private Information and demand security to safeguard their Private Information, took reasonable steps to maintain the confidentiality of their PII.

31. Defendant derived a substantial economic benefit from collecting Plaintiff's and Class Members' Private Information. In addition, obtaining, collecting, using, and deriving a benefit from Plaintiff's and Class Members' Private Information, Defendant assumed legal and equitable duties, and knew or should have known that it was responsible for protecting Plaintiff's and Class Members' Private Information from disclosure.

32. At all times material, Defendant was under a duty to adopt and implement reasonable measures to protect the Private Information of Plaintiff and Class Members from involuntary disclosure to third parties. And to that end, Defendant also has a legal duty created by contract, industry standards, and representations made to Plaintiff and Class Members, to keep their Private Information confidential and to protect it from unauthorized access and disclosure. Given the highly sensitive nature of the PII it possessed and the sensitivity of the services it provides, Defendant had a duty to safeguard, protect, and encrypt Plaintiff's and Class Members' PII.

33. By obtaining, collecting, storing, and transmitting the Private Information of Plaintiff and Class Members, Defendant assumed legal and equitable duties and knew or should have known that they were responsible for protecting the Private Information from disclosure.

34. Plaintiff and Class Members have taken reasonable steps to maintain the confidentiality of their Private Information and relied on Defendant to keep their Private Information confidential and maintained securely, to use this information for business purposes only, and to make only authorized disclosures of this information.

35. Defendant, via its Privacy Policy, expressly promised to maintain and protect their Private Information, demonstrating an understanding of the importance of securing Private Information.

36. Defendant's negligence in safeguarding the Private Information of Plaintiff and Class Members is exacerbated by the repeated warnings and alerts directed to protecting and securing sensitive data.

37. Defendant was not permitted to disclose Plaintiff's and Class Members' Private Information for any reason that would apply in this situation. The disclosure of Plaintiff's and Class Members' Private Information via the Data Breach was not permitted per Defendant's own privacy notice.

38. Defendant failed to use reasonable security procedures and practices appropriate to safeguard the sensitive, unencrypted information it was maintaining of Plaintiff and Class Members, consequently enabling and causing the exposure of Private Information of approximately 1.1 million individuals.

39. Because of Defendant's negligence and misconduct in failing to keep their information confidential, the unencrypted Private Information of Plaintiff and Class Members has been expropriated by unauthorized individuals who can now access the PII of Plaintiff and Class Members and use it as they please.

40. Plaintiff and Class Members now face a real, present and substantially increased risk of fraud and have lost the benefit of the bargain they made with Defendant when receiving services.

Data Breaches Lead to Identity Theft and Cognizable Injuries.

41. The PII of consumers, such as Plaintiff and Class Members, is valuable and has been commoditized in recent years.

42. Defendant was also aware of the significant repercussions that would result from its failure to do protect Private Information and knew, or should have known, the importance of safeguarding the Private Information entrusted to it and of the foreseeable consequences in the event of a breach of its data security. Nonetheless, Defendant failed to take adequate cybersecurity measures to prevent the Data Breach from occurring.

43. Identity theft associated with data breaches is particularly pernicious due to the fact that the information is made available, and has usefulness to identity thieves, for an extended period of time after it is stolen. As a result, victims suffer both immediate and long-lasting exposure and are susceptible to further injury over the passage of time.

44. As a direct and proximate result of Defendant's conduct, Plaintiff and the other Class Members have been placed at an imminent, immediate, and continuing increased risk of harm from fraud and identity theft. They must now be vigilant and continuously review their credit reports for suspected incidents of identity theft, educate themselves about security freezes, fraud alerts, and take steps to protect themselves against identity theft, which will extend indefinitely into the future.

45. Even absent any adverse use, consumers suffer injury from the simple fact that Private Information has been stolen. When such sensitive information is stolen, accounts become less secure, and the information once used to sign up for bank accounts and other financial services is no longer as reliable as it had been before the theft. Thus, consumers must spend time and money to re-secure their financial position and rebuild the good standing they once had in the community.

46. Plaintiff and the other Class Members have also suffered ascertainable losses in the form of opportunity costs and the time and costs reasonably incurred to remedy or mitigate the effects of the Data Breach, including:

A. Monitoring compromised accounts for fraudulent charges;

B. Canceling and reissuing credit and debit cards linked to the financial information in possession of Defendant;

C. Purchasing credit monitoring and identity theft prevention;

D. Addressing their inability to withdraw funds linked to compromised accounts;

E. Taking trips to banks and waiting in line to obtain funds held in limited accounts;

F. Taking trips to banks and waiting in line to verify their identities in order to restore access to the accounts;

G. Placing freezes and alerts with credit reporting agencies;

H. Spending time on the phone with or at financial institutions to dispute fraudulent charges;

I. Contacting their financial institutions and closing or modifying financial accounts;

J. Resetting automatic billing and payment instructions from compromised credit and debit cards to new cards;

K. Paying late fees and declined payment fees imposed as a result of failed automatic payments that were tied to compromised accounts that had to be cancelled; and,

L. Closely reviewing and monitoring financial accounts and credit reports for unauthorized activity for years to come.

47. Moreover, Plaintiff and the other Class Members have an interest in ensuring that Defendant implement reasonable security measures and safeguards to maintain the integrity and confidentiality of the Private Information, including making sure that the storage of data or documents containing Private Information is not accessible by unauthorized persons, that access to such data is sufficiently protected, and that the Private Information remaining in the possession of Defendant is fully secure, remains secure, and is not subject to future theft.

48. As a further direct and proximate result of Defendant's actions and inactions, Plaintiff and the other Class Members have suffered anxiety, emotional distress, and loss of privacy, and are at an increased risk of future harm.

49. As a direct and proximate result of Defendant's wrongful actions or omissions here, resulting in the Data Breach and the unauthorized release and disclosure of Plaintiff's and other Class Members' Private Information, Plaintiff and all Class Members have suffered, and will continue to suffer, ascertainable losses, economic damages, and other actual injury and harm,

including, *inter alia*, (i) the resulting increased and imminent risk of future ascertainable losses, economic damages and other actual injury and harm, (ii) the opportunity cost and value of lost time they must spend to monitor their financial accounts and other personal accounts—for which they are entitled to compensation; and (iii) emotional distress as a result of having their Private Information accessed and exfiltrated in the Data Breach.

Dell Was Well Aware of the Threat of Cyber Theft and Exfiltration

50. As a condition of its relationships with its clients, customers, and Class Members, Defendant required that they entrust it with highly sensitive and confidential PII and financial information. Defendant, in turn, collected that information and assured consumers that it was acting to protect that PII and to prevent its disclosure.

51. Defendant could have prevented the Data Breach by assuring that the Private Information at issue was properly secured.

52. Defendant's overt negligence in safeguarding Plaintiff's and Class Members' PII is exacerbated by repeated warnings and alerts directed to protecting and securing sensitive data, as evidenced by the trending data breach attacks in recent years. Further, as an entity that collects consumer financial and payment information, and provides consumer credit through Dell Pay, Defendant was on notice that such companies are targets for data breach hackers and cyber-thieves.

53. PII, including names and social security numbers are uniquely valuable to hackers. With these pieces of information, criminals can open new financial accounts in Class Member's names, take loans in their names, use their names to obtain medical services, obtain government benefits, file fraudulent tax returns in order to get refunds to which they are not even entitled, and numerous other assorted acts of thievery and fraud.

54. Social Security numbers are among the most sensitive kind of personal information. They are difficult for an individual to change. 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 potential misuse of a Social Security number is not permitted; an individual instead must show evidence of actual, ongoing fraud to obtain a new number.[8]

55. A new Social Security number may not be effective. According to Julie Ferguson of the Identity Theft Resource Center, "The credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[9]

56. For this reason, hackers prey on companies that collect and maintain sensitive financial information, including financial institutions, tax servicers, insurers, and related entities. Companies like Defendant have been aware of this, and the need to take adequate measures to secure their systems and information, for a number of years. In 2021 alone, approximately 279 breaches targeting financial service providers occurred.[10] That figure represented a substantial increase from the year before and the year before that.[11] The steady growth of hacks of financial services providers is no surprise and can be tied to two significant factors, (1) the failure of financial services providers, like Defendant, to adequately protect patient data and (2) the substantial value of the sensitive PII entrusted to financial service providers.

57. In 2021, 1,862 data breaches occurred, resulting in approximately 164,683,455 sensitive records being exposed, an increase of 68% over 2020 and a 23% increase over the previous all-time high.[12] These data breaches exposed the sensitive data of approximately 294 million people. *Id.* Hackers are increasingly targeting highly sensitive PII, including social

---

8 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-millions worrying-about-identity-theft (last accessed May 31, 2024)

9 *Id.*

10 ITRC_2021_Data_Breach_Report.pdf (idtheftcenter.org) at 6. (last visited on May 31, 2024).

11 *Id.*

12 ITRC_2021_Data_Breach_Report.pdf (idtheftcenter.org) (last visited on May 31, 2024)

security numbers and, in 2021, approximately 1,136 data breaches exposed social security numbers. *Id.*

58. Companies like Dell are well aware of the risk that data breaches pose to consumers, especially because both the size of their customer base and the fact that the PII that they collect and maintain is profoundly valuable to hackers. Indeed, Federal Reserve Chairman Jerome Powell has referred to cyber-attacks as the number one threat to the global financial system.[13]

59. It can be inferred from the Data Breach that Defendant either failed to implement, or inadequately implemented, information security policies or procedures in place to protect Representative Plaintiff's and Class Members' PII.

60. Upon information and belief, prior to the Data Breach, Defendant was aware of its security failures but failed to correct them or to disclose them to the public, including Plaintiff and Class Members.

61. The implementation of proper data security processes requires affirmative acts. Accordingly, Defendant knew or should have known that it did not make such actions and failed to implement adequate data security practices.

62. Because Defendant has failed to comply with industry standards, while monetary relief may cure some of Plaintiff's and Class Members' injuries, injunctive relief is necessary to ensure Defendant's approach to information security is adequate and appropriate. Defendant still maintains the PII of Plaintiff and Class Members; and without the supervision of the Court via injunctive relief, Representative Plaintiff's and Class Members' PII remains at risk of subsequent data breaches.

63. In addition to its obligations under state and common laws, Defendant owed a duty to Plaintiff and Class Members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the PII in Defendant's possession from being compromised,

[13] For Financial Institutions, Cyberthreats Loom Large (forbes.com) (last visited May 7, 2024)

lost, stolen, accessed, and misused by unauthorized persons. Defendant owed a duty to Plaintiff and Class Members to provide reasonable security, including consistency with industry standards and requirements, and to ensure that its computer systems, networks, and protocols adequately protected the Private Information of Plaintiff and Class Members.

64. Defendant owed a duty to Plaintiff and Class Members to ensure that the Private Information it collected and was responsible for was adequately secured and protected.

65. Defendant owed a duty to Plaintiff and Class Members to create and implement reasonable data security practices and procedures to protect the PII and financial information in its possession, including not sharing information with other entities who maintained sub-standard data security systems.

66. Defendant owed a duty to Plaintiff and Class Members to implement processes that would immediately detect a breach that impacted the Private Information it collected and was responsible for in a timely manner.

67. Defendant owed a duty to Plaintiff and Class Members to act upon data security warnings and alerts in a timely fashion.

68. Defendant owed a duty to Plaintiff and Class Members to disclose if its data security practices were inadequate to safeguard individuals' Private Information from theft because such an inadequacy would be a material fact in the decision to entrust this Private Information to Defendant.

69. Defendant owed a duty of care to Plaintiff and Class Members because they were foreseeable and probable victims of any inadequate data security practices.

70. Defendant owed a duty to Plaintiff and Class Members to mitigate the harm suffered by the Representative Plaintiff and Class Members as a result of the Data Breach.

Dell Violated FTC Guidelines Prohibiting Unfair or Deceptive Acts

71. The Federal Trade Commission Act, 15 U.S.C. § 45 ("FTC Act") prohibits businesses from engaging in "unfair or deceptive acts or practices in or affecting commerce." The

FTC has concluded that a company's failure to maintain reasonable and appropriate data security for consumers' sensitive personal information is an "unfair practice" in violation of the FTC Act. *See e.g., FTC v. Wyndham Corp.*, 799 F.3d 236 (3d Cir. 2015).

72. The FTC has promulgated numerous guides for businesses that highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.[14]

73. The FTC provided cybersecurity guidelines for businesses, advising that businesses should protect personal customer information, properly dispose of personal information that is no longer needed, encrypt information stored on networks, understand their network's vulnerabilities, and implement policies to correct any security problems.[15]

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

75. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the FTC Act. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

76. Defendant failed to properly implement basic data security practices. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to consumer PII constitutes an unfair act or practice prohibited by Section 5 of the FTC Act.

---

[14] https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf (last visited May 31, 2024).

[15] https://www.ftc.gov/business-guidance/resources/protecting-personal-information-guide-business (last visited May 31, 2024).

77. Defendant was at all times fully aware of its obligations to protect Plaintiff's and Class Members' Private Information because of its business model of collecting Private Information and storing such information. Defendant was also aware of the significant repercussions that would result from its failure to do so.

Value of the Relevant Sensitive Information

78. The high value of PII and financial information to criminals is evidenced by the prices they garner on 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.[16] Experian reports that a stolen credit or debit card number can sell for $5 to $110 on the dark web.[17] Criminals can also purchase access to entire company data breaches from $999 to $4,995.[18]

79. These criminal activities have and will result in devastating financial and personal losses to Plaintiff and Class Members. For example, it is believed that certain PII compromised in the 2017 Experian data breach was being used, three years later, by identity thieves to apply for COVID-19-related benefits in the state of Oklahoma. Such fraud will be an omnipresent threat for Plaintiff and Class Members for the rest of their lives. They will need to remain constantly vigilant.

80. The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority." The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, Social Security number, date of birth, official State or government issued driver's license or identification number,

---

16 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-darkweb-how-much-it-costs/ (last accessed May 31, 2024).

17 *Id*.

18 In the Dark, VPNOverview, 2019, available at: https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/ (last accessed May 31, 2024).

alien registration number, government passport number, employer or taxpayer identification number."

81. Identity thieves can use PII and financial information, such as that of Plaintiff and Class Members, which Defendant failed to keep secure, to perpetrate a variety of crimes that harm victims. For instance, identity thieves may commit various types of government fraud such as immigration fraud, obtaining a driver's license or identification card in the victim's name but with another's picture, using the victim's information to obtain government benefits, or filing a fraudulent tax return using the victim's information to obtain a fraudulent refund.

82. The ramifications of Defendant's failure to keep secure Plaintiff's and Class Members' PII are long lasting and severe. Once PII and financial information is stolen, particularly identification numbers, fraudulent use of that information and damage to victims may continue for years. Indeed, the PII of Plaintiff and Class Members was taken by hackers to engage in identity theft or to sell it to other criminals who will purchase the PII for that purpose. The fraudulent activity resulting from the Data Breach may not come to light for years.

83. There may be a time lag between when harm occurs versus when it is discovered, and also between when PII and/or financial information is stolen and when it is used. According to the U.S. Government Accountability Office ("GAO"), which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[19]

[19] 47 Report to Congressional Requesters, GAO, at 29 (June 2007), available at: http://www.gao.gov/new.items/d07737.pdf (last accessed May 31, 2024).

84. Data breaches are preventable.[20] As Lucy Thompson wrote in the DATA BREACH AND ENCRYPTION HANDBOOK, "[i]n almost all cases, the data breaches that occurred could have been prevented by proper planning and the correct design and implementation of appropriate security solutions."[21] She added that "[o]rganizations that collect, use, store, and share sensitive personal data must accept responsibility for protecting the information and ensuring that it is not compromised."[22]

85. Most of the reported data breaches are a result of lax security and the failure to create or enforce appropriate security policies, rules, and procedures … Appropriate information security controls, including encryption, must be implemented and enforced in a rigorous and disciplined manner so that a *data breach never occurs*."[23]

Defendant's Delayed Response to the Breach

86. Time is of the essence when highly sensitive PII is subject to unauthorized access and/or acquisition. The disclosed, accessed, and/or acquired PII of Plaintiff and Class Members is likely available on the Dark Web. Hackers can access and then offer for sale the unencrypted, unredacted PII to criminals. Plaintiff and Class Members are now subject to the present and continuing risk of fraud, identity theft, and misuse resulting from the possible publication of their PII onto the Dark Web. Plaintiff and Class Members now face a lifetime risk of identity theft, which is heightened here by unauthorized access, disclosure, and/or activity by cybercriminals on computer systems containing the critical PII of millions of consumers.

87. Despite this understanding, Defendant has not timely informed affected individuals, including Plaintiff and Class Members, about the Data Breach.

---

20 Lucy L. Thompson, Despite the Alarming Trends, Data Breaches Are Preventable, in DATA BREACH AND ENCRYPTION HANDBOOK (Lucy Thompson, ed., 2012)

21 *Id*. at 17.

22 *Id*. at 28.

23 *Id.*

88. Time is a compensable and valuable resource in the United States. According to the U.S. Bureau of Labor Statistics, 55.6% of U.S.-based workers are compensated on an hourly basis, while the other 44.5% are salaried.[24]

89. According to the U.S. Bureau of Labor Statistics' 2022 American Time Use Survey, American adults have only 36 to 40 hours of "leisure time" outside of work per week;[25] leisure time is defined as time not occupied with work or chores and is "the time equivalent of 'disposable income.'"[26] Usually, this time can be spent at the option and choice of the consumer, however, having been notified of the Data Breach, consumers now have to spend hours of their leisure time self-monitoring their accounts, communicating with financial institutions and government entities, and placing other prophylactic measures in place to attempt to protect themselves.

90. Plaintiff and Class Members are now deprived of the choice as to how to spend their valuable free hours and seek remuneration for the loss of valuable time as another element of damages.

CLASS ALLEGATIONS

91. Pursuant to Fed. R. Civ. P. 23(b)(1), (b)(2), (b)(3), and (c)(4), Plaintiff asserts common law claims, as more fully alleged hereinafter, on behalf of the following Nationwide Class. In addition, Plaintiff asserts common law claims, as more fully alleged hereinafter, on behalf of a Washington Class, defined as follows:

> **Nationwide Class**: All residents of the United States whose PII was accessed or otherwise compromised as a result of the Data Breach.

---

[24] U.S. BUREAU OF LABOR STATISTICS, Wage Worker Survey, available at https://www.bls.gov/opub/reports/minimum-wage/2022/home.htm (last visited May 31, 2024); see also U.S. BUREAU OF LABOR STATISTICS, Employment And Average Hourly Earnings By Industry, available at https://www.bls.gov/news.release/empsit.t19.htm (last visited May 31, 2024) (finding that on average, private-sector workers make $1,166.20 per 40-hour work week).

[25] See https://www.cnbc.com/2019/11/06/how-successful-people-spend-leisure-time-james-wallman.html?&qsearchterm=James%20Wallman (last visited May 31, 2024).

[26] *Id.*

Washington Class: All residents of the State of Washington whose PII was accessed or otherwise compromised as a result of the Data Breach.

Members of the Nationwide Class and the Washington Class are referred to herein collectively as "Class Members" or "Class."

92. Excluded from the Class are Defendant, any entity in which Defendant have a controlling interest, and Defendant's officers, directors, legal representatives, successors, subsidiaries, and assigns. Also excluded from the Class is any judge, justice, or judicial officer presiding over this matter and the members of their immediate families and judicial staff.

93. The proposed Class meets the requirements of Fed. R. Civ. P. 23(a), (b)(1), (b)(2), (b)(3), and (c)(4).

94. **Numerosity**: The exact number of members of the Class is unknown to Plaintiff at this time but Defendant provides services to millions of consumers throughout the United States and has acknowledged that approximately 49 consumers were impacted by the Data Breach. Ultimately, members of the Class will be readily identified through Defendant's records.

95. **Commonality and Predominance**: There are many questions of law and fact common to the claims of Plaintiff and the other members of the Class, and those questions predominate over any questions that may affect individual members of the Class. Common questions for the Class include:

a) Whether Defendant failed to adequately safeguard Plaintiff's and the Class Members' PII;

b) Whether Defendant failed to protect Plaintiff's and the Class Members' PII, as promised;

c) Whether Defendant's computer system systems and data security practices used to protect Plaintiff's and the Class Members' PII violated federal, state, and local laws, or Defendant's duties;

d) Whether Defendant engaged in unfair, unlawful, or deceptive practices by

failing to safeguard Plaintiff's and the Class Members' PII properly and/or as promised;

e) Whether Defendant violated the consumer protection statutes, data breach notification statutes, state unfair practice statutes, state privacy statutes, and/or FTC law or regulations, imposing duties upon Defendant, applicable to Plaintiff and Class Members;

f) Whether Defendant failed to notify Plaintiff and members of the Class about the Data Breach as soon as practical and without delay after the Data Breach was discovered;

g) Whether Defendant acted negligently in failing to safeguard Plaintiff's and the Class Members' PII;

h) Whether Defendant entered into contracts that included contract terms requiring Defendant to protect the confidentiality of Plaintiff's PII and have reasonable security measures;

i) Whether Defendant's conduct described herein constitutes a breach of their contracts benefiting Plaintiff and each of the Class Members;

j) Whether Defendant should retain the money paid by Plaintiff and each of the Class Members to protect their PII;

k) Whether Plaintiff and the Class Members are entitled to damages as a result of Defendant's wrongful conduct;

l) Whether Plaintiff and the Class Members are entitled to restitution as a result of Defendant's wrongful conduct;

m) What equitable relief is appropriate to redress Defendant's wrongful conduct; and

n) What injunctive relief is appropriate to redress the imminent and currently ongoing harm faced by Class Members.

96. **Typicality**: Plaintiff's claims are typical of the claims of each of the Class Members. Plaintiff and the Class Members sustained damages as a result of Defendant's uniform wrongful conduct during transactions with them.

97. **Adequacy**: Plaintiff will fairly and adequately represent and protect the interests of the Class, and have retained counsel competent and experienced in complex litigation and class actions. Plaintiff has no interests antagonistic to those of the Class, and there are no defenses unique to Plaintiff. Plaintiff and her counsel are committed to prosecuting this action vigorously on behalf of the members of the proposed Class, and have the financial resources to do so. Neither Plaintiff nor her counsel have any interest adverse to those of the other members of the Class.

98. **Separateness**: This case is appropriate for certification because prosecution of separate actions would risk either inconsistent adjudications which would establish incompatible standards of conduct for the Defendant or would be dispositive of the interests of members of the proposed Class. Furthermore, the Private Information collected by Defendant still exists, and is still vulnerable to future attacks – one standard of conduct is needed to ensure the future safety of the PII of Plaintiff and Class Members.

99. **Class-wide Applicability**: This case is appropriate for certification because Defendant has acted or refused to act on grounds generally applicable to the Plaintiff and proposed Class as a whole, thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct towards members of the Class, and making final injunctive relief appropriate with respect to the proposed Class as a whole. Defendant's practices challenged herein apply to and affect the members of the Class uniformly, and Plaintiff's challenge to those practices hinges on Defendant's conduct with respect to the proposed Class as a whole, not on individual facts or law applicable only to Plaintiff.

100. **Superiority**: This case is also appropriate for certification because class proceedings are superior to all other available means of fair and efficient adjudication of the claims of Plaintiff and the members of the Class. The injuries suffered by each individual member of the Class are relatively small in comparison to the burden and expense of individual prosecution of

the litigation necessitated by Defendant's conduct. Absent a class action, it would be virtually impossible for individual members of the Class to obtain effective relief from Defendant. Even if Class Members could sustain individual litigation, it would not be preferable to a class action because individual litigation would increase the delay and expense to all parties, including the Court, and would require duplicative consideration of the common legal and factual issues presented here. By contrast, a class action presents far fewer management difficulties and provides the benefits of single adjudication, economies of scale, and comprehensive supervision by a single Court.

COUNT I

Negligence
(On Behalf of Plaintiff and the Nationwide Class and Washington Class)

101. Plaintiff, on behalf of herself and the Class, re-alleges and incorporates the above allegations by reference.

102. Plaintiff and Class Members were required to submit PII to Defendant, in order to obtain services.

103. Defendant knew, or should have known, of the risks and responsibilities inherent in collecting and storing the PII of Plaintiff and Class Members.

104. As described above, Defendant owed a duty of care to Plaintiff and Class Members whose PII had been entrusted to Defendant.

105. Defendant breached its duty to Plaintiff and Class Members by failing to secure the PII that Defendant collected from consumers from unauthorized disclosure to third parties.

106. Defendant acted with wanton disregard for the security of Plaintiff's and Class Members' PII.

107. A "special relationship" exists between Defendant and the Plaintiff and Class Members. Defendant entered into a "special relationship" with Plaintiff and Class Members because it collected and/or stored the PII of Plaintiff and the Class Members.

108. But for Defendant's wrongful and negligent breach of its duty owed to Plaintiff and the Class Members, Plaintiff and the Class Members would not have been injured.

109. The injury and harm suffered by Plaintiff and Class Members was the reasonably foreseeable result of Defendant's breach of its duty. Defendant knew or should have known it was failing to meet its duty, and that Defendant's breach of such duties would cause Plaintiff and Class Members to experience the foreseeable harms associated with the unauthorized exposure of their PII.

110. As a direct and proximate result of Defendant's negligent conduct, Plaintiff and Class Members have suffered injury and are entitled to damages in an amount to be proven at trial.

COUNT II

Negligence *Per Se*
(On Behalf of Plaintiff and the Nationwide Class and Washington Class)

111. Plaintiff, on behalf of herself and the Class, re-alleges and incorporates the above allegations by reference.

112. Pursuant to the FTC Act (15 U.S.C. § 45, *et seq*.), Defendant had a duty to implement reasonable safeguards to protect Plaintiff's and Class Members' PII.

113. Defendant breached its duty to Plaintiff and Class Members by failing to implement reasonable safeguards to protect Plaintiff's and Class Members' PII from unauthorized access.

114. Defendant's failure to comply with applicable laws and regulations constitutes negligence *per se*.

115. But for Defendant's wrongful and negligent breach of its duty owed to Plaintiff and Class Members, Plaintiff and Class Members would not have been injured.

116. The injury and harm suffered by Plaintiff and Class Members was the reasonably foreseeable result of Defendant's breach of its duties. Defendant knew or should have known that it was failing to meet its duty, and that Defendant's breach of that duty would cause Plaintiff and

Class Members to experience the foreseeable harms associated with the unauthorized access to their PII.

117. On information and belief, as a direct and proximate result of Defendant's negligent conduct, Plaintiff and Class Members have suffered injury and are entitled to damages in an amount to be proven at trial.

COUNT III

Breach of Implied Covenant of Good Faith and Fair Dealing (On Behalf of Plaintiff and the Nationwide Class and Washington Class)

118. Plaintiff, on behalf of herself and the Class, re-alleges and incorporates the above allegations by reference.

119. Plaintiff and Class Members entered into valid, binding, and enforceable express or implied contracts with entities affiliated with or serviced by Defendant, as alleged above.

120. The contracts respecting which Plaintiff and Class Members were intended beneficiaries were subject to implied covenants of good faith and fair dealing that all parties would act in good faith and with reasonable efforts to perform their contractual obligations (both explicit and fairly implied) and not to impair the rights of the other parties to receive the rights, benefits, and reasonable expectations under the contracts. These included the implied covenants that Defendant would act fairly and in good faith in carrying out its contractual obligations to take reasonable measures to protect Plaintiff's PII from unauthorized disclosure and to comply with state laws and regulations.

121. A "special relationship" exists between Defendant and the Plaintiff and Class Members. Defendant entered into a "special relationship" with Plaintiff and Class Members who sought services from Defendant and, in doing so, entrusted Defendant, pursuant to its requirements and Privacy Notice, with their PII.

122. Despite this special relationship with Plaintiff, Defendant did not act in good faith and with fair dealing to protect Plaintiff's and Class Members' PII.

123. Plaintiff and Class Members performed all conditions, covenants, obligations, and promises owed to Defendant.

124. Defendant's failure to act in good faith in complying with the contracts denied Plaintiff and Class Members the full benefit of their bargain, and instead they received services that were less valuable than what they paid for and less valuable than their reasonable expectations.

125. Accordingly, on information and belief, Plaintiff and Class Members have been injured as a result of Defendant's breach of the covenant of good faith and fair dealing respecting which they are express or implied beneficiaries, and are entitled to damages and/or restitution in an amount to be proven at trial.

COUNT IV

Breach of Duty
(On Behalf of Plaintiff and the Nationwide Class and Washington Class)

126. Plaintiff, on behalf of herself and the Class, re-alleges and incorporates the above allegations by reference.

127. Defendant accepted the special confidence placed in it by Plaintiff and Class Members. There was an understanding between the parties that Defendant would act for the benefit of Plaintiff and Class Members in preserving the confidentiality of their PII.

128. Defendant became the guardian of Plaintiff's and Class Members' PII and accepted a fiduciary duty to act primarily for the benefit of its patients, including Plaintiff and the Class Members, including safeguarding Plaintiff's and the Class Members' PII.

129. Defendant breached its fiduciary duty to Plaintiff and Class Members by (a) failing to protect the PII of Plaintiff and the Class; (b) by failing to notify Plaintiff and the Class Members of the unauthorized disclosure of the PII; and (c) by otherwise failing to safeguard Plaintiff's and the Class Members' PII.

130. As a direct and proximate result of Defendant's breach of its fiduciary duty, Plaintiff and/or Class Members have suffered and/or will suffer injury, including but not limited

to: (a) the compromise of their PII; and (b) the diminished value of the services they received as a result of unauthorized exposing of Plaintiff's and Class Members' PII.

131. On information and belief, as a direct and proximate result of Defendant's breach of its fiduciary duty, Plaintiff and Class Members have suffered and will continue to suffer other forms of injury and/or harm, and other economic and non-economic losses.

COUNT V

Breach of Implied Contract
(On Behalf of Plaintiff and the Nationwide Class and Washington Class)

132. Plaintiff, on behalf of herself and the Class, re-alleges and incorporates by reference herein all of the allegations contained above.

133. Defendant collected and maintained responsibility for the Private Information of Plaintiff and the Class, including, *inter alia*, name, date of birth, address, Social Security Number, and other PII in connection with the provision of services to Plaintiff and the Class.

134. At the time Defendant acquired the PII of Plaintiff and the Class, there was a meeting of the minds and a mutual understanding that Defendant would safeguard the PII and not take unjustified risks when storing the PII.

135. Plaintiff and the Class would not have entrusted their PII to Defendant had they known that Defendant would fail to adequately safeguard their PII.

136. Prior to the Data Breach, Defendant published the Privacy Notice, agreeing to protect and keep private financial information of Plaintiff and the Class.

137. Implicit in the agreement between Plaintiff and Class Members and the Defendant to provide PII, was the latter's obligation to: (a) use such PII for business purposes only, (b) take reasonable steps to safeguard that PII, (c) prevent unauthorized disclosures of the PII, (d) provide

Plaintiff and Class Members with prompt and sufficient notice of any and all unauthorized access and/or theft of their PII, (e) reasonably safeguard and protect the PII of Plaintiff and Class Members from unauthorized disclosure or uses, and (f) retain the PII only under conditions that kept such information secure and confidential.

138. In collecting and maintaining responsibility for the maintenance and protection of the PII of Plaintiff and the Class and publishing the Privacy Notice, Defendant entered into contracts with Plaintiff and the Class requiring Defendant to protect and keep secure the PII of Plaintiff and the Class.

139. Plaintiff and the Class fully performed their obligations under the contracts with Defendant.

140. Defendant breached the contracts they made with Plaintiff and the Class by failing to protect and keep private financial information of Plaintiff and the Class.

141. On information and belief, as a direct and proximate result of Defendant's above-described breach of implied contract, Plaintiff and the Class have suffered (and will continue to suffer) ongoing, imminent, and impending threat of identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; loss of the confidentiality of the stolen confidential data; the illegal sale of the compromised data on the dark web; expenses and/or time spent on credit monitoring and identity theft insurance; additional time spent scrutinizing bank statements, credit card statements, and credit reports; expenses and/or time spent initiating fraud alerts, credit freezes, decreased credit scores and ratings; lost work time; and other economic and non-economic harm.

142. As a direct and proximate result of Defendant's breach of contract, Plaintiff and the

Class are at an increased risk of identity theft or fraud.

143. As a direct and proximate result of Defendant's breach of contract, Plaintiff is entitled to and demand actual, consequential, and nominal damages and injunctive relief, to be determined at trial.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff on behalf of herself and the proposed Class, prays for relief and judgment against Defendant as follows:

A. certifying the Class pursuant to Rule 23 of the Federal Rules of Civil Procedure, appointing Plaintiff as representative of the Class, and designating Plaintiff's counsel as Class Counsel;

B. declaring that Defendant's conduct violates the laws referenced herein;

C. finding in favor of Plaintiff and the Class on all counts asserted herein;

D. awarding Plaintiff and the Class compensatory damages and actual damages, trebled, in an amount exceeding $5,000,000, to be determined by proof;

E. awarding Plaintiff and the Class appropriate relief, including actual, nominal and statutory damages;

F. awarding Plaintiff and the Class punitive damages;

G. awarding Plaintiff and the Class civil penalties;

H. granting Plaintiff and the Class declaratory and equitable relief, including restitution and disgorgement;

I. enjoining Defendant from continuing to engage in the wrongful acts and practices alleged herein;

J. awarding Plaintiff and the Class the costs of prosecuting this action, including expert witness fees;

K. awarding Plaintiff and the Class reasonable attorneys' fees and costs as allowable

by law;

L. awarding pre-judgment and post-judgment interest; and

M. granting any other relief as this Court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiff demands a trial by jury on all triable issues.

DATED: June 11, 2024

Respectfully submitted,

/s/ Bruce W. Steckler
Bruce W. Steckler
Texas Bar I.D. 00785039
STECKLER WAYNE & LOVE PLLC
12720 Hillcrest Road, Suite 1045
Dallas, TX 75230
Telephone: (972) 387-4040
Facsimile: (972) 387-4041
bruce@swclaw.com

BARRACK, RODOS & BACINE
STEPHEN R. BASSER *
SAMUEL M. WARD*
600 West Broadway, Suite 900
San Diego, CA 92101
Telephone: (619) 230-0800
Facsimile: (619) 230-1874
sbasser@barrack.com
sward@barrack.com

Counsel for Plaintiff and the Class

**Pro Hac Vice* application to be filed