UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK

FREDERICK CONAWAY and TINA QAMAR, individually and on behalf of all others similarly situated, Plaintiffs, v. CSC SERVICEWORKS, INC., Defendant.	Case No.: 2:24-cv-05719-JMA-ARL CONSOLIDATED CLASS ACTION COMPLAINT JURY TRIAL DEMANDED

Plaintiffs Frederick Conaway and Tina Qamar ("Plaintiffs"), individually and on behalf of all others similarly situated, and on behalf of the general public, bring this Consolidated Class Action Complaint, against defendant CSC ServiceWorks, Inc. ("CSC ServiceWorks" or "Defendant") based on personal knowledge and the investigation of counsel, and alleges as follows:

I. INTRODUCTION

1. With this action, Plaintiffs seek to hold Defendant responsible for the harms it caused Plaintiffs and similarly situated persons in the preventable data breach of Defendant's inadequately protected computer network.

2. Defendant is a company that offers technology platforms for laundry services, tire inflation services, and vacuum services to customers across the country.

3. As part of its business, and in order to gain profits, Defendant obtained and stored the personal information of Plaintiffs and Class members.

4. By taking possession and control of Plaintiffs' and Class members' personal information, Defendant assumed a duty to securely store and protect it.

5. Defendant breached this duty and betrayed the trust of Plaintiffs and Class members by failing to properly safeguard and protect their personal information, thus enabling cybercriminals to access, acquire, appropriate, compromise, disclose, encumber, exfiltrate, release, steal, misuse, and/or view it.

6. On or about February 4, 2024, CSC ServiceWorks detected suspicious activity on its computer network, indicating a data breach. Based on a subsequent forensic investigation, CSC ServiceWorks determined that cybercriminals infiltrated its inadequately secured computer systems and thereby gained access to its data files (the "Data Breach"). The investigation further determined that, through this infiltration, cybercriminals potentially accessed and acquired files containing the sensitive personal information of 35,340 individuals.[1]

7. According to CSC ServiceWorks, the personal information accessed by cybercriminals involved a wide variety of personally identifiable information ("PII"), including but not limited to names, dates of birth, Social Security numbers, contact information, driver's license numbers, financial account information, health insurance information, and medical information (collectively, "Personal Information").

8. Defendant's misconduct – failing to implement adequate and reasonable measures to protect Plaintiffs' and Class members' Personal Information, failing to timely detect the Data Breach, failing to take adequate steps to prevent and stop the Data Breach, failing to disclose the material facts that it did not have adequate security practices in place to safeguard the Personal Information, and failing to provide timely and adequate notice of the Data Breach – caused substantial harm and injuries to Plaintiffs and Class members across the United States.

[1] *See* https://www.maine.gov/agviewer/content/ag/985235c7-cb95-4be2-8792-a1252b4f8318/2d81a065-2d73-4bcf-8deb-92365996681d.html.

9. Due to Defendant's negligence and failures, cyber criminals obtained and now possess everything they need to commit personal identity theft and wreak havoc on the financial and personal lives of thousands of individuals, for decades to come.

10. Plaintiffs bring this class action lawsuit to hold Defendant responsible for its grossly negligent—indeed, reckless—failure to use statutorily required or reasonable industry cybersecurity measures to protect Class members' Personal Information.

11. As a result of the Data Breach, Plaintiffs and Class members have already suffered damages. For example, now that their Personal Information has been released into the criminal cyber domains, Plaintiffs and Class members are at imminent and impending risk of identity theft. This risk will continue for the rest of their lives, as Plaintiffs and Class members are now forced to deal with the danger of identity thieves possessing and using their Personal Information.

12. Additionally, Plaintiffs and Class members have already lost time and money responding to and mitigating the impact of the Data Breach, which efforts are continuous and ongoing.

13. Plaintiffs bring this action individually and on behalf of the Class and seeks actual damages and restitution. Plaintiffs also seek declaratory and injunctive relief, including significant improvements to Defendant's data security systems and protocols, future annual audits, Defendant-funded long-term credit monitoring services, and other remedies as the Court sees necessary and proper.

14. Defendant's failure to timely report and provide Plaintiffs and the Class Members with notice of the Data Breach made the victims vulnerable to identity theft without any warnings to monitor their financial accounts or credit reports to prevent unauthorized use of their PII.

15. Defendant knew or should have known that each victim of the Data Breach

deserved prompt and efficient notice of the Data Breach and assistance in mitigating the effects of PII misuse.

16. Defendant disregarded the rights of Plaintiffs and Class Members by intentionally, willfully, recklessly, and/or negligently failing to take and implement adequate and reasonable measures to ensure that the PII of Plaintiffs and Class Members 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, the Plaintiffs' and Class Members' PII was compromised through disclosure to an unknown and unauthorized criminal third party.

17. Upon information and belief, cybercriminals were able to breach Defendant's systems because Defendant breached its duties and obligations in one or more of the following ways: (1) failing to design or being negligent in the design, implementation, monitor, and maintaining reasonable network safeguards against foreseeable threats; (2) failing to design, implement, and maintain reasonable data retention policies; (3) failing to adequately train staff on data security; (4) failing to comply with industry-standard data security practices; (5) failing to warn Plaintiffs and Class Members of Defendant's inadequate data security practices; (6) failing to encrypt or adequately encrypt the PII; (7) failing to recognize or detect that its network had been compromised and accessed in a timely manner to mitigate the harm; (8) failing to utilize widely available software able to detect and prevent this type of attack; and (9) otherwise failing to secure the hardware using reasonable and effective data security procedures free of foreseeable vulnerabilities and data security incidents. These failures rendered Riverside an easy target for cybercriminals.

18. In failing to adequately protect individuals' information or adequately notify them

about the breach, and by obfuscating the nature of the breach, Defendant violated state law and harmed a staggering number of customers and/or employees.

19. Plaintiffs and the Class Members are victims of Defendant's negligence and inadequate cyber security measures. Specifically, Plaintiffs and members of the proposed Class trusted Defendant with their PII, but Defendant betrayed that trust. Defendant failed to properly use reasonable industry standard security practices to prevent the Data Breach.

20. The exposure of one's PII to cybercriminals is a bell that cannot be unrung. Before the Data Breach, the Personal Information of Plaintiffs and the Class was exactly that—private. Not anymore. Now, their Personal Information is permanently exposed and unsecure.

II. THE PARTIES

21. Plaintiff Conaway is a citizen and resident of Gwinnett County, Georgia.

22. Plaintiff Qamar is a citizen and resident of Kendall County, Illinois.

23. Defendant CSC ServiceWorks, Inc. is a corporation organized under the state laws of Florida with its principal place of business located in Melville, New York.

III. JURISDICTION AND VENUE

24. Plaintiffs incorporate by reference all allegations of the preceding paragraphs as though fully set forth herein.

25. This Court has diversity jurisdiction over this action under the Class Action Fairness Act (CAFA), 28 U.S.C. § 1332(d) because this is a class action involving more than 100 class members, the amount in controversy exceeds $5,000,000, exclusive of interest and costs, and Plaintiffs and members of the Class are citizens of states that differ from Defendant.

26. This Court has personal jurisdiction over Defendant because Defendant conducts business in this District, maintains its principal place of business in this District, and has sufficient minimum contacts this State.

27. Venue is likewise proper as to Defendant in this District under 28 U.S.C. § 1391(a)(1) because Defendant's principal place of business is in this District and therefore resides in this District pursuant to 28 U.S.C. § 1391(c)(2). Venue is further proper in this District under 28 U.S.C. § 1391(b)(2) because a substantial part of the events or omissions giving rise to the Class's claims also occurred in this District.

IV. FACTUAL ALLEGATIONS

A. The Data Breach, Defendant's Belated Notice, and Defendant's Lax Data Security

28. On or about February 4, 2024, CSC ServiceWorks detected suspicious activity on its computer network, indicating a data breach. Based on a subsequent forensic investigation, CSC ServiceWorks determined that cybercriminals infiltrated its inadequately secured computer systems and thereby gained access to its data files between September 23, 2023 and February 4, 2024. The investigation further determined that, through this infiltration, cybercriminals potentially accessed and acquired files containing the sensitive personal information of 35,340 individuals.[2]

29. According to the breach letters sent by CSC ServiceWorks, the Personal Information accessed by cybercriminals involved a wide variety of PII, including but not limited to names, dates of birth, Social Security numbers, contact information, driver's license numbers, financial account information, health insurance information, and medical information.

30. Despite the breadth and sensitivity of the PII that was exposed, and the attendant consequences to affected individuals as a result of the exposure, Defendant failed to disclose the Data Breach for several months from the time of the Breach. This inexplicable delay further exacerbated the harms to Plaintiffs and Class members.

[2] *See* https://www.maine.gov/agviewer/content/ag/985235c7-cb95-4be2-8792-a1252b4f8318/2d81a065-2d73-4bcf-8deb-92365996681d.html.

31. Based on the notice letter received by Plaintiffs, the type of cyberattack involved, and public news reports, it is plausible and likely that Plaintiffs' Personal Information was stolen in the Data Breach.

32. Upon information and belief, the unauthorized third-party cybercriminal gained access to the Personal Information, exfiltrated the Personal Information from Defendant's network, and has engaged in (and will continue to engage in) misuse of the Personal Information, including marketing and selling Plaintiffs' and Class members' Personal Information on the dark web.

33. Accordingly, Defendant had obligations created by industry standards, common law, statutory law, and its own assurances and representations to keep Plaintiffs and Class members' Personal Information confidential and to protect such Personal Information from unauthorized access.

34. On information and belief, Defendant failed to adequately train and supervise its IT and data security agents and employees on reasonable cybersecurity protocols or implement reasonable security measures, causing it to lose control over its employees' and/or customers' PII. Defendant's negligence is evidenced by its failure to prevent the Data Breach and stop cybercriminals from accessing the PII.

35. For example, as evidenced by the Data Breach's occurrence, the infiltrated network was not protected by sufficient multi-layer data security technologies or effective firewalls.

36. Similarly, despite the fact that unauthorized cybercriminals had accessed Defendant's network in September 2023, Defendant did not detect this unauthorized access until February 2024, according to their own admissions. Based on the months-long delayed discovery of the Data Breach, it is evident that the infiltrated network, that Defendant allowed to store Plaintiffs' PII, did not have sufficiently effective endpoint detection.

37. Further, the fact that PII was acquired in the Data Breach demonstrates that the PII contained in the Defendant's network was not encrypted. Had the information been properly encrypted, the data thieves would have exfiltrated only unintelligible data.

38. Plaintiffs and Class Members entrusted Defendant with sensitive and confidential information, including their PII, which includes information (such as Social Security numbers) that are static, do not change, and can be used to commit a myriad of financial crimes.

39. Even with several months of credit monitoring services, the risk of identity theft and unauthorized use of Plaintiffs' and Class Members' PII is still substantially high. The fraudulent activity resulting from the Data Breach may not come to light for years.

40. Nevertheless, Defendant failed to spend sufficient resources on preventing external access, detecting outside infiltration, and training its employees to identify email-borne threats and defend against them.

41. The stolen Personal Information at issue has great value to the hackers, due to the large number of individuals affected and the fact the sensitive information that was part of the data that was compromised.

42. The Data Breach at issue here is not the only example of CSC ServiceWorks' lax data security practices. Earlier this year, it was widely published that two UC Santa Cruz students, Alexander Sherbrooke and Iakov Taranenko, exploited a security vulnerability in Defendant's system that "allowed anyone to remotely send commands to laundry machines run by CSC and operate laundry cycles for free."[3] According to the report:

> Since CSC ServiceWorks lacked a dedicated security page for reporting security vulnerabilities, Sherbrooke and Taranenko *sent the company several messages through its online contact form in January but heard nothing back. A phone call to the company landed them nowhere either, they said*. [Emphasis added.]

[3] https://www.darkreading.com/ics-ot-security/students-spot-washing-machine-app-flaw-that-gives-out-free-cycles

43. In other words, even after the students advised Defendant of the security flaw, CSC ServiceWorks did not acknowledge its vulnerability.

44. The Data Breach reflects a similar lack of concern by Defendant. The vulnerabilities that led to the Breach could have, and should have, been detected and remedied. However, Defendant failed in its obligations to Plaintiffs and the Class.

B. Plaintiffs' Experiences

Plaintiff Conaway

45. Plaintiff Conaway is a former employee of CSC ServicesWorks.

46. As a condition of his employment with Defendant, Plaintiff Conaway was required to supply Defendant with her Personal Information, including her full name and Social Security number.

47. Plaintiff Conaway received a notice letter from Defendant dated August 9, 2024, informing him that his Personal Information—including his Social Security Number—was specifically identified as having been exposed to cybercriminals in the Data Breach.

48. Plaintiff Conaway is very careful with his Personal Information and, to the best of his knowledge, has never before been a victim of a data breach.

49. Because of the Data Breach, Plaintiff's Personal Information is now in the hands of cyber criminals. Plaintiff Conaway and all Class members are now imminently at risk of crippling future identity theft and fraud.

50. Plaintiff Conaway has suffered actual injury from the exposure and theft of his Personal Information—which violates his right to privacy.

51. Since the Data Breach, Plaintiff Conaway has experienced identity theft in the form of unauthorized transactions on this financial account. Plaintiff Conaway attributes the foregoing

suspicious and unauthorized activity to the Data Breach given the time proximity, the fact that his financial account information was identified as having been exposed in the Data Breach, the fact that he has never experienced anything like this prior to now, and, to his knowledge, his Personal Information has never been exposed in any other Data Breach.

52. In addition, since the Data Breach, Plaintiff Conaway has experienced a noticeable and considerable increase in spam phone calls and robocalls.

53. As a result of the Data Breach, Plaintiff Conaway has already expended time and suffered loss of productivity from taking time to address and attempt to ameliorate, mitigate, and address the future consequences of the Data Breach, including investigating the Data Breach, researching how best to ensure that he is protected from identity theft, reviewing account statements and other information, and taking other steps in an attempt to mitigate the harm caused by the Data Breach. This time has been lost forever and cannot be recaptured.

54. The letter Plaintiff Conaway received from Defendant specifically directed him to take the actions described above. Indeed, the breach notification letter advised Plaintiff Conaway and all Class Members that they should "remain vigilant for fraud or identity theft by reviewing your account statements and free credit reports."[4] In addition, the breach notification letter listed several "steps" that victims of the Data Breach should take to help protect themselves including, enrolling in credit monitoring, monitoring accounts, placing fraud alerts with credit reporting bureaus, placing security freezes on credit reports, filing a complaint with the FTC, and obtaining information about identity theft and frauds.[5]

[4] *See* Sample Breach letter, available at: https://www.maine.gov/agviewer/content/ag/985235c7-cb95-4be2-8792-a1252b4f8318/2d81a065-2d73-4bcf-8deb-92365996681d.html.

[5] *Id.*

55. As a result of the Data Breach, Plaintiff Conaway has experienced stress, anxiety, and concern due to the loss of his privacy and concern over the impact of cybercriminals accessing and misusing his Personal Information. Plaintiff Conaway fears that criminals will use his information to commit identity theft.

56. Plaintiff Conaway anticipates spending considerable time and money on an ongoing basis.

57. Plaintiff Conaway has also suffered injury directly and proximately caused by the Data Breach, including: (a) theft of Plaintiff's valuable Personal Information; (b) the imminent and certain impending injury flowing from fraud and identity theft posed by Plaintiff's Personal Information being placed in the hands of cybercriminals; (c) damages to and/or diminution in value of Plaintiff's Personal Information that was entrusted to Defendant with the understanding that Defendant would safeguard this information against disclosure; (d) loss of the benefit of the bargain with Defendant to provide adequate and reasonable data security—*i.e.*, the difference in value between what Plaintiff Conaway should have received from Defendant and Defendant's defective and deficient performance of that obligation by failing to provide reasonable and adequate data security and failing to protect Plaintiff's Personal Information; and (e) continued risk to Plaintiff's Personal Information, which remains in the possession of Defendant and which is subject to further breaches so long as Defendant fails to undertake appropriate and adequate measures to protect the Personal Information that was entrusted to Defendant.

Plaintiff Qamar

58. Plaintiff Qamar received a notice letter from Defendant dated August 9, 2024, informing her that her Personal Information—including her Social Security Number—was specifically identified as having been exposed to cybercriminals in the Data Breach.

59. Plaintiff Qamar is very careful with her Personal Information and, to the best of her knowledge, has never before been a victim of a data breach.

60. Because of the Data Breach, Plaintiff's Personal Information is now in the hands of cyber criminals. Plaintiff Qamar and all Class members are now imminently at risk of crippling future identity theft and fraud.

61. Plaintiff Qamar has suffered actual injury from the exposure and theft of her Personal Information—which violates her right to privacy.

62. Since the Data Breach, Plaintiff Qamar has experienced a surge of spam calls, texts and emails immediately following the Data Breach, which she describes as "a ton," and which continue to arrive weekly as of the date of this filing. Qamar believes and thereupon avers this surge in vexatious spamming was directly caused by the Data Breach, given the close time proximity and the unusual nature of the sudden uptick in calls, texts, and emails.

63. As a result of the Data Breach, Plaintiff Qamar has already expended time and suffered loss of productivity from taking time to address and attempt to ameliorate, mitigate, and address the future consequences of the Data Breach, including verifying the legitimacy and impact of the Data Breach, exploring credit monitoring and identity theft insurance options, self-monitoring her accounts and seeking legal counsel regarding her options for remedying and/or mitigating the effects of the Data Breach. This time has been lost forever and cannot be recaptured.

64. The letter Plaintiff Qamar received from Defendant specifically directed her to take the actions described above. Indeed, the breach notification letter advised Plaintiff Qamar and all Class Members that they should "remain vigilant for fraud or identity theft by reviewing your account statements and free credit reports."[6] In addition, the breach notification letter listed several

[6] *See* Sample Breach letter, available at: https://www.maine.gov/

"steps" that victims of the Data Breach should take to help protect themselves including, enrolling in credit monitoring, monitoring accounts, placing fraud alerts with credit reporting bureaus, placing security freezes on credit reports, filing a complaint with the FTC, and obtaining information about identity theft and frauds.[7]

65. As a result of the Data Breach, Plaintiff Qamar has experienced stress, anxiety, and concern due to the loss of her privacy and concern over the impact of cybercriminals accessing and misusing her Personal Information. Plaintiff Qamar fears that criminals will use her information to commit identity theft.

66. Plaintiff Qamar anticipates spending considerable time and money on an ongoing basis.

67. Plaintiff Qamar has also suffered injury directly and proximately caused by the Data Breach, including: (a) theft of Plaintiff's valuable Personal Information; (b) the imminent and certain impending injury flowing from fraud and identity theft posed by Plaintiff's Personal Information being placed in the hands of cybercriminals; (c) damages to and/or diminution in value of Plaintiff's Personal Information that was entrusted to Defendant with the understanding that Defendant would safeguard this information against disclosure; (d) loss of the benefit of the bargain with Defendant to provide adequate and reasonable data security—*i.e.*, the difference in value between what Plaintiff Qamar should have received from Defendant and Defendant's defective and deficient performance of that obligation by failing to provide reasonable and adequate data security and failing to protect Plaintiff's Personal Information; and (e) continued risk to Plaintiff's Personal Information, which remains in the possession of Defendant and which

agviewer/content/ag/985235c7-cb95-4be2-8792-a1252b4f8318/2d81a065-2d73-4bcf-8deb-92365996681d.html.

[7] *Id.*

is subject to further breaches so long as Defendant fails to undertake appropriate and adequate measures to protect the Personal Information that was entrusted to Defendant.

C. Common Injuries & Damages

68. As result of Defendant's ineffective and inadequate data security practices, Plaintiffs and Class Members now face a present and ongoing risk of fraud and identity theft.

69. Due to the Data Breach, and the foreseeable consequences of PII ending up in the possession of criminals, the risk of identity theft to Plaintiffs and Class Members has materialized and is imminent and continuing. Plaintiffs and Class Members have all sustained actual injuries and damages, including: (a) invasion of privacy; (b) "out of pocket" costs incurred mitigating the materialized risk and imminent threat of identity theft; (c) loss of time and loss of productivity incurred mitigating the materialized risk and imminent threat of identity theft risk; (d) "out of pocket" costs incurred due to actual identity theft; (e) loss of time incurred due to actual identity theft; (f) loss of time due to increased spam and targeted marketing emails; (g) the loss of benefit of the bargain (price premium damages); (h) diminution or loss of value of their PII; and (i) the continued risk to their PII, which remains in Defendant's possession, and which is subject to further breaches, so long as Defendant fail to undertake appropriate and adequate measures to protect Plaintiffs' and Class Members' PII.

The Risk of Identity Theft to Plaintiffs and Class Members Is Present and Ongoing

70. The link between a data breach and the risk of identity theft is simple and well established. Criminals acquire and steal PII to monetize the information. Criminals monetize the data by selling the stolen information on the black market to other criminals who then utilize the information to commit a variety of identity theft related crimes discussed below.

71. Because a person's identity is akin to a puzzle with multiple data points, the more

accurate pieces of data an identity thief obtains about a person, the easier it is for the thief to take on the victim's identity – or track the victim to attempt other hacking crimes against the individual to obtain more data to perfect a crime.

72. For example, armed with just a name and date of birth, a data thief can utilize a hacking technique referred to as "social engineering" to obtain even more information about a victim's identity, such as a person's login credentials or Social Security number. Social engineering is a form of hacking whereby a data thief uses previously acquired information to manipulate and trick individuals into disclosing additional confidential or personal information through means such as spam phone calls and text messages or phishing emails. Data breaches are often the starting point for these additional targeted attacks on the victims.

73. The Dark Web is an unindexed layer of the internet that requires special software or authentication to access.[8] Criminals in particular favor the Dark Web as it offers a degree of anonymity to visitors and website publishers. Unlike the traditional or 'surface' web, Dark Web users need to know the web address of the website they wish to visit in advance. For example, on the surface web, the CIA's web address is cia.gov, but on the Dark Web the CIA's web address is ciadotgov4sjwlzihbbgxnqg3xiyrg7so2r2o3lt5wz5ypk4sxyjstad.onion.[9] This prevents Dark Web marketplaces from being easily monitored by authorities or accessed by those not in the know.

74. A sophisticated black market exists on the Dark Web where criminals can buy or sell malware, firearms, drugs, and frequently, personal and medical information like the PII at issue here.[10] The digital character of PII stolen in data breaches lends itself to Dark Web

[8] Louis DeNicola, *What Is the Dark Web?*, Experian (May 12, 2021), https://www.experian.com/blogs/ask-experian/what-is-the-dark-web/ (last visited Dec. 7, 2023).
[9] *Id.*
[10] *What is the Dark Web?* – Microsoft 365 (July 15, 2022), https://www.microsoft.com/en-us/microsoft-365-life-hacks/privacy-and-safety/what-is-the-dark-web (last visited Dec. 7, 2023).

transactions because it is immediately transmissible over the internet and the buyer and seller can retain their anonymity. The sale of a firearm or drugs on the other hand requires a physical delivery address. Nefarious actors can readily purchase usernames and passwords for online streaming services, stolen financial information and account login credentials, Social Security numbers, dates of birth, and medical information.[11] As Microsoft warns "[t]he anonymity of the dark web lends itself well to those who would seek to do financial harm to others."[12]

75. Social Security numbers, for example, are among the worst kind of personal information to have stolen because they may be put to numerous serious 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.[13]
>
> What's 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.

76. Even then, new a Social Security number may not be effective, as "[t]he credit bureaus and banks are able to link the new number very quickly to the old number, so all of that

---

[11] *Id.*; *see also* Louis DeNicola, *supra*.
[12] *Id.*
[13] Social Security Administration, *Identity Theft and Your Social Security Number* (2021), available at: https://www.ssa.gov/pubs/EN-05-10064.pdf (last visited Dec. 7, 2023).

old bad information is quickly inherited into the new Social Security number."[14]

77. Identity thieves can also use Social Security numbers to obtain a driver's license or official identification card in the victim's name but with the thief's picture; use the victim's name and Social Security number to obtain government benefits; or file a fraudulent tax return using the victim's information. In addition, identity thieves may obtain a job using the victim's Social Security number, rent a house or receive medical services in the victim's name, and may even give the victim's personal information to police during an arrest resulting in an arrest warrant being issued in the victim's name. And the Social Security Administration has warned that identity thieves can use an individual's Social Security number to apply for additional credit lines.[15]

78. According to the FBI's Internet Crime Complaint Center (IC3) 2019 Internet Crime Report, Internet-enabled crimes reached their highest number of complaints and dollar losses that year, resulting in more than $3.5 billion in losses to individuals and business victims.[16]

79. Further, according to the same report, "rapid reporting can help law enforcement stop fraudulent transactions before a victim loses the money for good."[17] Defendant did not rapidly report to Plaintiffs and Class Members that their PII had been stolen.

80. 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.

81. In addition to out-of-pocket expenses that can exceed thousands of dollars and the

---

[14] Brian Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR (Feb. 9, 2015), http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millions-worrying-about-identity-theft (last visited Dec. 7, 2023).

[15] *Identity Theft and Your Social Security Number*, Social Security Administration, 1 (2021), https://www.ssa.gov/pubs/EN-05-10064.pdf (last visited Dec. 7, 2023).

[16] *See 2019 Internet Crime Report*, FBI (Feb. 11, 2020), https://www.fbi.gov/news/stories/2019-internet-crime-report-released-021120 (last visited Dec. 7, 2023).

[17] *Id.*

emotional toll identity theft can take, some victims have to spend a considerable time repairing the damage caused by the theft of their PII. Victims of new account identity theft will likely have to spend time correcting fraudulent information in their credit reports and continuously monitor their reports for future inaccuracies, close existing bank/credit accounts, open new ones, and dispute charges with creditors.

82. Further complicating the issues faced by victims of identity theft, data thieves may wait years before attempting to use the stolen PII. To protect themselves, Plaintiffs and Class Members will need to remain vigilant against unauthorized data use for years or even decades to come.

83. The Federal Trade Commission ("FTC") has also recognized that consumer data is a new and valuable form of currency. In an FTC roundtable presentation, former Commissioner Pamela Jones Harbour stated that "most consumers cannot begin to comprehend the types and amount of information collected by businesses, or why their information may be commercially valuable. Data is currency. The larger the data set, the greater potential for analysis and profit."[18]

84. The FTC has also issued numerous guidelines for businesses that highlight the importance of reasonable data security practices. The FTC has noted the need to factor data security into all business decision-making. According to the FTC, data security requires: (1) encrypting information stored on computer networks; (2) retaining payment card information only as long as necessary; (3) properly disposing of personal information that is no longer needed; (4) limiting administrative access to business systems; (5) using industry-tested and accepted methods for securing data; (6) monitoring activity on networks to uncover unapproved activity; (7)

[18] Statement of FTC Commissioner Pamela Jones Harbour (Remarks Before FTC Exploring Privacy Roundtable), FTC (Dec. 7, 2009), http://www.ftc.gov/speeches/harbour/091207privacyroundtable.pdf (last visited Dec. 7, 2023).

verifying that privacy and security features function properly; (8) testing for common vulnerabilities; and (9) updating and patching third-party software.[19]

85. According to the FTC, unauthorized PII disclosures are extremely damaging to consumers' finances, credit history and reputation, and can take time, money, and patience to resolve the fallout. The FTC treats 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(a) of the FTC Act.[20]

86. Defendant's failure to properly notify Plaintiffs and Class Members of the Data Breach exacerbated Plaintiffs' and Class Members' injury by depriving them of the earliest ability to take appropriate measures to protect their PII and take other necessary steps to mitigate the harm caused by the Data Breach.

Loss of Time to Mitigate the Risk of Identify Theft and Fraud

87. As a result of the recognized risk of identity theft, when a Data Breach occurs, and an individual is notified by a company that their PII was compromised, as in this Data Breach, the reasonable person is expected to take steps and spend time to address the dangerous situation, learn about the breach, and otherwise mitigate the risk of becoming a victim of identity theft or fraud. Failure to spend time taking steps to review accounts or credit reports could expose the individual to greater financial harm – yet the resource and asset of time has been lost.

88. Thus, due to Defendant's admitted recognition of the actual and imminent risk of identity theft, Defendant offered Plaintiffs and Class Members abbreviated, non-automatic credit

[19] *See generally* https://www.ftc.gov/business-guidance/resources/protecting-personal-information-guide-business (last visited Dec. 7, 2023).
[20] *See, e.g.*, *Protecting Personal Information: A Guide for Business*, FTC, https://www.ftc.gov/news-events/news/press-releases/2016/07/commission-finds-labmd-liable-unfair-data-security-practices (last visited Dec. 7, 2023).

monitoring services.

89. Plaintiffs and Class Members have spent, and will spend additional time in the future, on a variety of prudent actions, such as placing "freezes" and "alerts" with credit reporting agencies, contacting financial institutions, closing or modifying financial accounts, changing passwords, reviewing and monitoring credit reports and accounts for unauthorized activity, and filing police reports, which may take years to discover and detect.

90. Plaintiffs' mitigation efforts are consistent with the U.S. Government Accountability Office that released a report in 2007 regarding data breaches ("GAO Report") in which it noted that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."[21]

91. Plaintiffs' mitigation efforts are also consistent with the steps that FTC recommends that data breach victims take to protect their personal and financial information after a data breach, including: contacting one of the credit bureaus to place a fraud alert (and consider an extended fraud alert that lasts for seven years if someone steals their identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.[22]

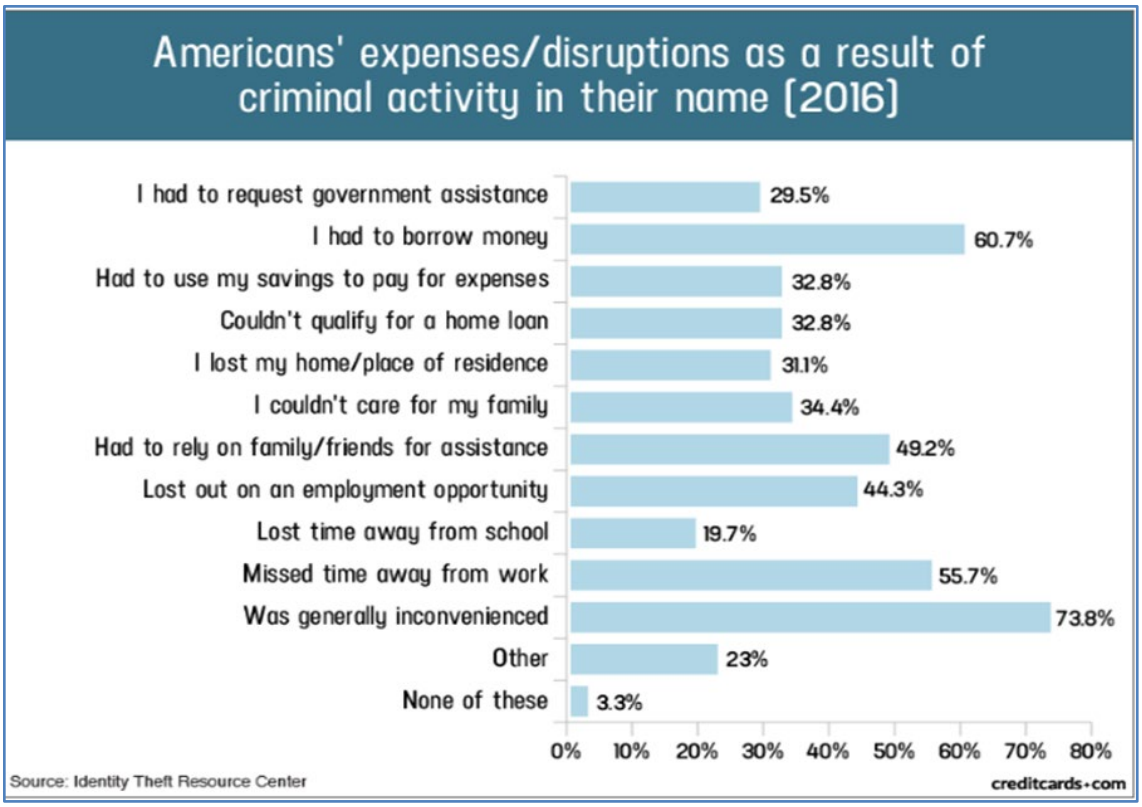
92. A study by Identity Theft Resource Center shows the multitude of harms caused by fraudulent use of personal and financial information:[23]

---

[21] *See* U.S. GOV'T ACCOUNTABILITY OFF., GAO-07-737, PERSONAL INFORMATION: DATA BREACHES ARE FREQUENT, BUT EVIDENCE OF RESULTING IDENTITY THEFT IS LIMITED; HOWEVER, THE FULL EXTENT IS UNKNOWN (2007) ("GAO Report"), available at https://www.gao.gov/new.items/d07737.pdf (last visited Dec. 7, 2023).

[22] *See* Federal Trade Commission, IdentityTheft.gov, https://www.identitytheft.gov/Steps (last visited Dec. 7, 2023).

[23] Credit Card and ID Theft Statistics" by Jason Steele, 10/24/2017, at: https://web.archive.org/web/20190304002224/https://www.creditcards.com/credit-card-news/credit-card-security-id-theft-fraud-statistics-1276.php (last visited Dec. 7, 2023).



93. Indeed, the FTC recommends that identity theft victims take several steps and spend time to protect their personal and financial information after a data breach, including contacting one of the credit bureaus to place a fraud alert (consider an extended fraud alert that lasts for 7 years if someone steals their identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.[24]

Diminution of Value of the PII

94. PII is a valuable property right.[25] Its value is axiomatic, considering the value of data in corporate America and the consequences of cyber thefts include heavy prison sentences.

[24] *See* Federal Trade Commission, IdentityTheft.gov, https://www.identitytheft.gov/Steps (last visited Dec. 7, 2023).

[25] *See, e.g.*, John T. Soma, et al, Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("PII") Equals the "Value" of Financial Assets, 15 Rich. J.L. & Tech. 11, at *3-4 (2009) ("PII, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets.") (citations omitted).

Even this obvious risk to reward analysis illustrates beyond a doubt that PII has considerable market value.

95. For example, drug manufacturers, medical device manufacturers, pharmacies, hospitals, and other healthcare service providers often purchase PII/PHI on the black market for the purpose of target-marketing their products and services to the physical maladies of the data breach victims themselves.

96. PII can sell for as much as $363 per record according to the Infosec Institute.[26]

97. Medical information is especially valuable to identity thieves. According to account monitoring company LogDog, medical data, such as PHI, sells for $50 and up on the Dark Web.[27]

98. An active and robust legitimate marketplace for PII also exists. In 2019, the data brokering industry was worth roughly $200 billion.[28] In fact, the data marketplace is so sophisticated that consumers can actually sell their non-public information directly to a data broker who in turn aggregates the information and provides it to marketers or app developers.[29, 30] Consumers who agree to provide their web browsing history to the Nielsen Corporation can receive up to $50.00 a year.[31]

99. As a result of the Data Breach, Plaintiffs' and Class Members' PII, which has an inherent market value in both legitimate and dark markets, has been damaged and diminished in

---

[26] *See* Ashiq Ja, *Hackers Selling Healthcare Data in the Black Market*, InfoSec (July 27, 2015), https://resources.infosecinstitute.com/topic/hackers-selling-healthcare-data-in-the-black-market/ (last visited Dec. 7, 2023).

[27] Lisa Vaas, *Ransomware Attacks Paralyze, and Sometimes Crush, Hospitals*, Naked Security (Oct. 3, 2019), https://nakedsecurity.sophos.com/2019/10/03/ransomware-attacks-paralyze-and-sometimes-crush-hospitals/#content (last visited Dec. 7, 2023).

[28] David Lazarus, *Column: Shadowy data brokers make the most of their invisibility cloak*, LA Times (Nov. 5, 2019), https://www.latimes.com/business/story/2019-11-05/column-data-brokers (last visited Dec. 7, 2023).

[29] https://datacoup.com (last visited Dec. 12, 2023).

[30] https://digi.me/how (last visited Dec. 12, 2023).

[31] Nielsen Computer & Mobile Panel, Frequently Asked Questions, available at https://computermobilepanel.nielsen.com/ui/US/en/faqen.html (last visited Dec. 7, 2023).

its value by its unauthorized and potential release onto the Dark Web, where it may soon be available and holds significant value for the threat actors.

Future Cost of Credit and Identity Theft Monitoring Is Reasonable and Necessary

100. To date, Defendant has done little to provide Plaintiffs and Class Members with relief for the damages they have suffered as a result of the Data Breach.

101. The abbreviated, non-automatic credit monitoring offered to persons whose PII was compromised is wholly inadequate as it fails to provide for the fact that victims of data breaches and other unauthorized disclosures commonly face ongoing identity theft and financial fraud for the remainder of their lives. Defendant also places the burden squarely on Plaintiffs and Class Members by requiring them to independently sign up for that service, as opposed to automatically enrolling all victims of this Data Breach.

102. Given the type of targeted attack in this case and sophisticated criminal activity, the type of PII, and the *modus operandi* of cybercriminals, there is a strong probability that entire batches of stolen information have been placed, or will be placed, on the black market/Dark Web for sale and purchase by criminals intending to utilize the PII for identity theft crimes – e.g., opening bank accounts in the victims' names to make purchases or to launder money; file false tax returns; take out loans or lines of credit; or file false unemployment claims.

103. It must be noted there may be a substantial time lag – measured in years – 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.

104. Such fraud may go undetected until debt collection calls commence months, or even years, later. An individual may not know that his or her Social Security Number was used to file for unemployment benefits until law enforcement notifies the individual's employer of the

suspected fraud. Fraudulent tax returns are typically discovered only when an individual's authentic tax return is rejected.

105. Furthermore, the information accessed and disseminated in the Data Breach is significantly more valuable than the loss of, for example, credit card information in a retailer data breach, where victims can easily cancel or close credit and debit card accounts.[32] The information disclosed in this Data Breach is impossible to "close" and difficult, if not impossible, to change (such as Social Security numbers).

106. Consequently, Plaintiffs and Class Members are at a present and ongoing risk of fraud and identity theft for many years into the future.

107. The retail cost of credit monitoring and identity theft monitoring can cost around $200 a year, or more, per Class Member. This is a reasonable and necessary cost to protect Class Members from the risk of identity theft that arose from Defendant's Data Breach. This is a future cost for a minimum of five years that Plaintiffs and Class Members would not need to bear but for Defendant's failure to safeguard their PII.

Injunctive Relief Is Necessary to Protect against Future Data Breaches

108. Moreover, Plaintiffs and Class Members have an interest in ensuring that their PII, which is believed to remain in the possession of Defendants, is protected from further breaches by the implementation of security measures and safeguards, including but not limited to, making sure that the storage of data or documents containing PII is not accessible online and that access to such data is password protected.

[32] *See* Jesse Damiani, *Your Social Security Number Costs $4 On The Dark Web, New Report Finds*, FORBES (Mar. 25, 2020), https://www.forbes.com/sites/jessedamiani/2020/03/25/your-social-security-number-costs-4-on-the-dark-web-new-report-finds/?sh=6a44b6d513f1 (last visited Dec. 7, 2023).

D. Defendant had an Obligation to Protect Personal Information under the Law and the Applicable Standard of Care

109. Defendant also prohibited by the Federal Trade Commission Act (the "FTC Act") (15 U.S.C. § 45) from engaging in "unfair or deceptive acts or practices in or affecting commerce." The Federal Trade Commission (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 Worldwide Corp.*, 799 F.3d 236 (3d Cir. 2015).

110. Defendant is further required by various states' laws and regulations to protect Plaintiffs' and Class members' Personal Information.

111. Defendant owed a duty to Plaintiffs and the Class to design, maintain, and test its computer and application systems to ensure that the Personal Information in its possession was adequately secured and protected.

112. Defendant owed a duty to Plaintiffs and the Class to create and implement reasonable data security practices and procedures to protect the Personal Information in its possession, including adequately training its employees (and others who accessed Personal Information within its computer systems) on how to adequately protect Personal Information.

113. Defendant owed a duty to Plaintiffs and the Class to implement processes that would detect a breach on its systems in a timely manner.

114. Defendant owed a duty to Plaintiffs and the Class to act upon data security warnings and alerts in a timely fashion.

115. Defendant owed a duty to Plaintiffs and the Class to disclose if its computer systems and data security practices were inadequate to safeguard individuals' Personal Information from

theft because such an inadequacy would be a material fact in the decision to entrust Personal Information with Defendant.

116. Defendant owed a duty to Plaintiffs and the Class to disclose in a timely and accurate manner when data breaches occurred.

117. Defendant owed a duty of care to Plaintiffs and the Class because it was a foreseeable victim of a data breach.

E. Defendant was on Notice of Cyber Attack Threats and of the Inadequacy of their Data Security

118. Data security breaches have dominated the headlines for the last two decades. And it doesn't take an IT industry expert to know it. The general public can tell you the names of some of the biggest cybersecurity breaches: Target,[33] Yahoo,[34] Marriott International,[35] Chipotle, Chili's, Arby's,[36] and others.[37]

119. Defendant should certainly have been aware, and indeed was aware, that it was at risk for a data breach that could expose the Personal Information that it collected and maintained.

120. Defendant was also on notice of the importance of data encryption of Personal Information. Defendant knew it kept Personal Information in its systems and yet it appears Defendant did not encrypt these systems or the information contained within them.

---

[33] Michael Kassner, *Anatomy of the Target Data Breach: Missed Opportunities and Lessons Learned*, ZDNET (Feb. 2, 2015), https://www.zdnet.com/article/anatomy-of-the-target-data-breach-missed-opportunities-and-lessons-learned/.

[34] Martyn Williams, *Inside the Russian Hack of Yahoo: How They Did It*, CSOONLINE.COM (Oct. 4, 2017), https://www.csoonline.com/article/3180762/inside-the-russian-hack-of-yahoo-how-they-did-it.html.

[35] Patrick Nohe, *The Marriot Data Breach: Full Autopsy*, THE SSL STORE: HASHEDOUT (Mar. 22, 2019), https://www.thesslstore.com/blog/autopsying-the-marriott-data-breach-this-is-why-insurance-matters/.

[36] Alfred Ng, *FBI Nabs Alleged Hackers in Theft of 15M Credit Cards from Chipotle, Others*, CNET (Aug. 1, 2018), https://www.cnet.com/news/fbi-nabs-alleged-hackers-in-theft-of-15m-credit-cards-from-chipotle-others/?ftag=CMG-01-10aaa1b.

[37] *See, e.g.*, Taylor Armerding, *The 18 Biggest Data Breaches of the 21st Century*, CSO ONLINE (Dec. 20, 2018), https://www.csoonline.com/article/2130877/the-biggest-data-breaches-of-the-21st-century.html.

F. Cyber Criminals Will Use Plaintiffs' and Class Members' Personal Information to Defraud Them

121. Plaintiffs and Class members' Personal Information is of great value to hackers and cyber criminals, and the data stolen in the Data Breach has been used and will continue to be used in a variety of sordid ways for criminals to exploit Plaintiffs and the Class members and to profit off their misfortune.

122. Each year, identity theft causes tens of billions of dollars of losses to victims in the United States.[38] For example, with the Personal Information stolen in the Data Breach, identity thieves can open financial accounts, apply for credit, collect government benefits, commit crimes, create false driver's licenses and other forms of identification and sell them to other criminals or undocumented immigrants, steal benefits, give breach victims' names to police during arrests, and many other harmful forms of identity theft.[39] These criminal activities have and will result in devastating financial and personal losses to Plaintiffs and Class members.

123. Personal Information is such a valuable commodity to identity thieves that once it has been compromised, criminals will use it and trade the information on the cyber black-market for years.[40]

124. Based on the foregoing, the information compromised in the Data Breach is significantly more valuable than the loss of, for example, credit card information in a retailer data breach because there, victims can cancel or close credit and debit card accounts. The information

---

[38] "Facts + Statistics: Identity Theft and Cybercrime," Insurance Info. Inst., https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime (discussing Javelin Strategy & Research's report "2018 Identity Fraud: Fraud Enters a New Era of Complexity").

[39] https://www.experian.com/blogs/ask-experian/what-should-i-do-if-my-drivers-license-number-is-stolen/.

[40] *Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown*, GAO, July 5, 2007, https://www.gao.gov/products/gao-07-737.

compromised in this Data Breach is impossible to "close" and difficult, if not impossible, to change—Social Security number and name.

125. This data demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "Compared to credit card information, personally identifiable information and Social Security numbers are worth more than 10x on the black market."[41]

126. This was a financially motivated Data Breach, as apparent from the discovery of the cyber criminals seeking to profit off the sale of Plaintiffs' and the Class members' Personal Information on the dark web. The Personal Information exposed in this Data Breach are valuable to identity thieves for use in the kinds of criminal activity described herein.

127. These risks are both certainly impending and substantial. As the FTC has reported, if hackers get access to personally identifiable information, they will use it.[42]

128. Hackers may not use the accessed information right away. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches:

> [I]n some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[43]

---

[41] Tim 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.

[42] Ari Lazarus, *How fast will identity thieves use stolen info?*, FED. TRADE COMM'N (May 24, 2017), https://www.consumer.ftc.gov/blog/2017/05/how-fast-will-identity-thieves-use-stolen-info.

[43] *Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown*, GAO, July 5, 2007, https://www.gao.gov/products/gao-07-737.

129. As described above, identity theft victims must spend countless hours and large amounts of money repairing the impact to their credit.[44]

130. With this Data Breach, identity thieves have already started to prey on the victims, and one can reasonably anticipate this will continue.

131. Victims of the Data Breach, like Plaintiffs and other Class members, must spend many hours and large amounts of money protecting themselves from the current and future negative impacts to their credit because of the Data Breach.[45]

132. In fact, as a direct and proximate result of the Data Breach, Plaintiffs and the Class have suffered, and have been placed at an imminent, immediate, and continuing increased risk of suffering, harm from fraud and identity theft. Plaintiffs and the Class must now take the time and effort and spend the money to mitigate the actual and potential impact of the Data Breach on their everyday lives, including purchasing identity theft and credit monitoring services, placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, healthcare providers, closing or modifying financial accounts, and closely reviewing and monitoring bank accounts, credit reports, and health insurance account information for unauthorized activity for years to come.

133. Plaintiffs and the Class have suffered, and continue to suffer, actual harms for which they are entitled to compensation, including:

a. Trespass, damage to, and theft of their personal property including Personal Information;

b. Improper disclosure of their Personal Information;

---

[44] "Guide for Assisting Identity Theft Victims," Federal Trade Commission, 4 (Sept. 2013), http://www.consumer.ftc.gov/articles/pdf-0119-guide-assisting-id-theft-victims.pdf.

[45] *Id.*

c. The imminent and certainly impending injury flowing from potential fraud and identity theft posed by their Personal Information being placed in the hands of criminals and having been already misused;

d. The imminent and certainly impending risk of having their Personal Information used against them by spam callers to defraud them;

e. Damages flowing from Defendant's untimely and inadequate notification of the data breach;

f. Loss of privacy suffered as a result of the Data Breach;

g. Ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably expended to remedy or mitigate the effects of the data breach;

h. Ascertainable losses in the form of deprivation of the value of individuals' personal information for which there is a well-established and quantifiable national and international market;

i. The loss of use of and access to their credit, accounts, and/or funds;

j. Damage to their credit due to fraudulent use of their Personal Information; and

k. Increased cost of borrowing, insurance, deposits and other items which are adversely affected by a reduced credit score.

134. Moreover, Plaintiffs and Class members have an interest in ensuring that their information, which remains in the possession of Defendant, is protected from further breaches by the implementation of industry standard and statutorily compliant security measures and

safeguards. Defendant has shown itself to be incapable of protecting Plaintiffs' and Class members' Personal Information.

135. Plaintiffs and Class members are desperately trying to mitigate the damage that Defendant has caused them but, given the Personal Information Defendant made accessible to hackers, they are certain to incur additional damages. Because identity thieves have their Personal Information, Plaintiffs and all Class members will need to have identity theft monitoring protection for the rest of their lives.

136. None of this should have happened. The Data Breach was preventable.

G. Defendant Could Have Prevented the Data Breach but Failed to Adequately Protect Plaintiffs' and Class Members' Personal Information

137. Data breaches are preventable.[46] 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."[47] 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 . . . ."[48]

138. "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*."[49]

---

[46] Lucy L. Thompson, "Despite the Alarming Trends, Data Breaches Are Preventable," *in* DATA BREACH AND ENCRYPTION HANDBOOK (Lucy Thompson, ed., 2012).
[47] *Id.* at 17.
[48] *Id.* at 28.
[49] *Id.*

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

140. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established cyber-security guidelines for businesses. The guidelines note that businesses should protect the personal customer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct any security problems.7 The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.[50]

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

142. 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 Federal Trade Commission Act ("FTCA"), 15

[50] *Protecting Personal Information: A Guide for Business*, Federal Trade Commission (2016). Available at https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf.

U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

143. Defendant failed to properly implement basic data security practices, including those set forth by the FTC.

144. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to customers' Personal Information constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

145. Defendant also failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework Version 2.0 (including without limitation PR.AA-01, PR.AA.-02, PR.AA-03, PR.AA-04, PR.AA-05, PR.AT-01, PR.DS-01, PR-DS-02, PR.DS-10, PR.PS-01, PR.PS-02, PR.PS-05, PR.IR-01, DE.CM-01, DE.CM-03, DE.CM-06, DE.CM-09, and RS.CO-04), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

146. Defendant was entrusted with properly holding, safeguarding, and protecting against unlawful disclosure of Plaintiffs' and Class Members' Personal Information.

147. Many failures laid the groundwork for the success ("success" from a cybercriminal's viewpoint) of the Data Breach, starting with Defendant's failure to incur the costs necessary to implement adequate and reasonable cyber security procedures and protocols necessary to protect Plaintiffs' and Class members' Personal Information.

148. Defendant was at all times fully aware of its obligation to protect the Personal Information of Plaintiffs and Class members. Defendant was also aware of the significant repercussions that would result from its failure to do so.

149. Defendant maintained the Personal Information in a reckless manner. In particular, the Personal Information was maintained and/or exchanged, unencrypted, in Defendant's systems and were maintained in a condition vulnerable to cyberattacks.

150. Defendant knew, or reasonably should have known, of the importance of safeguarding Personal Information and of the foreseeable consequences that would occur if Plaintiffs' and Class members' Personal Information was stolen, including the significant costs that would be placed on Plaintiffs and Class members as a result of a breach.

151. The mechanism of the cyberattack and potential for improper disclosure of Plaintiffs' and Class members' Personal Information was a known risk to Defendant, and thus Defendant was on notice that failing to take necessary steps to secure Plaintiffs' and Class members' Personal Information from those risks left that information in a dangerous condition.

152. Defendant disregarded the rights of Plaintiffs and Class members by, *inter alia*, (i) intentionally, willfully, recklessly, or negligently failing to take adequate and reasonable measures to ensure that its business email accounts were protected against unauthorized intrusions; (ii) failing to disclose that it did not have adequately robust security protocols and training practices in place to adequately safeguard Plaintiffs' and Class members' Personal Information; (iii) failing to take standard and reasonably available steps to prevent the Data Breach; (iv) concealing the existence and extent of the Data Breach for an unreasonable duration of time; and (v) failing to provide Plaintiffs and Class members prompt and accurate notice of the Data Breach.

V. CLASS ACTION ALLEGATIONS

153. Plaintiffs incorporate by reference all allegations of the preceding paragraphs as though fully set forth herein.

154. Plaintiffs bring all claims as class claims under Federal Rule of Civil Procedure 23. Plaintiffs assert all claims on behalf of the Class, defined as follows:

> All persons residing in the United States whose Personal Information was compromised as a result of the Data Breach.

155. Plaintiffs reserve the right to amend the above definition or to propose subclasses in subsequent pleadings and motions for class certification.

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

157. **Numerosity:** The proposed Class is believed to be so numerous that joinder of all members is impracticable. The proposed Subclass is also believed to be so numerous that joinder of all members would be impractical.

158. **Typicality:** Plaintiffs' claims are typical of the claims of the Class. Plaintiffs and all members of the Class were injured through Defendant's uniform misconduct. The same event and conduct that gave rise to Plaintiffs' claims are identical to those that give rise to the claims of every other Class member because Plaintiffs and each member of the Class had their sensitive Personal Information compromised in the same way by the same conduct of Defendant.

159. **Adequacy:** Plaintiffs are an adequate representative of the Class because her interests do not conflict with the interests of the Class and proposed Subclass that she seeks to represent; Plaintiffs have retained counsel competent and highly experienced in data breach class action litigation; and Plaintiffs and Plaintiffs' counsel intend to prosecute this action vigorously. The interests of the Class will be fairly and adequately protected by Plaintiffs and Plaintiffs' counsel.

160. **Superiority:** A class action is superior to other available means of fair and efficient adjudication of the claims of Plaintiffs and the Class. The injury suffered by each individual Class

member is relatively small in comparison to the burden and expense of individual prosecution of complex and expensive litigation. It would be very difficult, if not impossible, for members of the Class individually to effectively redress Defendant's wrongdoing. Even if Class members could afford such individual litigation, the court system could not. Individualized litigation presents a potential for inconsistent or contradictory judgments. Individualized litigation increases the delay and expense to all parties, and to the court system, presented by the complex legal and factual issues of the case. By contrast, the class action device presents far fewer management difficulties and provides benefits of single adjudication, economy of scale, and comprehensive supervision by a single court.

161. **Commonality and Predominance:** There are many questions of law and fact common to the claims of Plaintiffs 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 engaged in the wrongful conduct alleged herein;

b. Whether Defendant failed to adequately safeguard Plaintiffs' and the Class's Personal Information;

c. Whether Defendant's email and computer systems and data security practices used to protect Plaintiffs' and Class members' Personal Information violated the FTC Act, and/or state laws and/or Defendant's other duties discussed herein;

d. Whether Defendant owed a duty to Plaintiffs and the Class to adequately protect their Personal Information, and whether it breached this duty;

e. Whether Defendant knew or should have known that its computer and network security systems and business email accounts were vulnerable to a data breach;

f. Whether Defendant's conduct, including its failure to act, resulted in or was the proximate cause of the Data Breach;

g. Whether Defendant breached contractual duties owed to Plaintiffs and the Class to use reasonable care in protecting their Personal Information;

h. Whether Defendant failed to adequately respond to the Data Breach, including failing to investigate it diligently and notify affected individuals in the most expedient time possible and without unreasonable delay, and whether this caused damages to Plaintiffs and the Class;

i. Whether Defendant continues to breach duties to Plaintiffs and the Class;

j. Whether Plaintiffs and the Class suffered injury as a proximate result of Defendant's negligent actions or failures to act;

k. Whether Plaintiffs and the Class are entitled to recover damages, equitable relief, and other relief;

l. Whether injunctive relief is appropriate and, if so, what injunctive relief is necessary to redress the imminent and currently ongoing harm faced by Plaintiffs and members of the Class and the general public;

m. Whether Defendant's actions alleged herein constitute gross negligence; and

n. Whether Plaintiffs and Class members are entitled to punitive damages.

VI. CAUSES OF ACTION

COUNT ONE

NEGLIGENCE

162. Plaintiffs incorporate by reference all allegations of the preceding paragraphs as though fully set forth herein.

163. Defendant solicited, gathered, and stored the Personal Information of Plaintiffs and the Class as part of the operation of its business.

164. Upon accepting and storing the Personal Information of Plaintiffs and Class members, Defendant undertook and owed a duty to Plaintiffs and Class members to exercise reasonable care to secure and safeguard that information and to use secure methods to do so.

165. Defendant had full knowledge of the sensitivity of the Personal Information, the types of harm that Plaintiffs and Class members could and would suffer if the Personal Information was wrongfully disclosed, and the importance of adequate security.

166. Plaintiffs and Class members were the foreseeable victims of any inadequate safety and security practices on the part of Defendant. Plaintiffs and the Class members had no ability to protect their Personal Information that was in Defendant's possession. As such, a special relationship existed between Defendant and Plaintiffs and the Class.

167. Defendant was well aware of the fact that cyber criminals routinely target large corporations through cyberattacks in an attempt to steal sensitive personal information.

168. Defendant owed Plaintiffs and the Class members a common law duty to use reasonable care to avoid causing foreseeable risk of harm to Plaintiffs and the Class when obtaining, storing, using, and managing personal information, including taking action to reasonably safeguard such data and providing notification to Plaintiffs and the Class members of any breach in a timely manner so that appropriate action could be taken to minimize losses.

169. Defendant's duty extended to protecting Plaintiffs and the Class from the risk of foreseeable criminal conduct of third parties, which has been recognized in situations where the actor's own conduct or misconduct exposes another to the risk or defeats protections put in place to guard against the risk, or where the parties are in a special relationship. *See* Restatement (Second) of Torts § 302B. Numerous courts and legislatures also have recognized the existence of a specific duty to reasonably safeguard personal information.

170. Defendant had duties to protect and safeguard the Personal Information of Plaintiffs and the Class from being vulnerable to cyberattacks by taking common-sense precautions when dealing with sensitive Personal Information. Additional duties that Defendant owed Plaintiffs and the Class include:

a. To exercise reasonable care in designing, implementing, maintaining, monitoring, and testing Defendant's networks, systems, email accounts, protocols, policies, procedures and practices to ensure that Plaintiffs' and Class members' Personal Information was adequately secured from impermissible release, disclosure, and publication;

b. To protect Plaintiffs' and Class members' Personal Information in its possession by using reasonable and adequate security procedures and systems;

c. To implement processes to quickly detect a data breach, security incident, or intrusion involving its business email system, networks and servers; and

d. To promptly notify Plaintiffs and Class members of any data breach, security incident, or intrusion that affected or may have affected their Personal Information.

171. Only Defendant was in a position to ensure that its systems and protocols were sufficient to protect the Personal Information that Plaintiffs and the Class had entrusted to it.

172. Defendant breached its duty of care by failing to adequately protect Plaintiffs' and Class members' Personal Information. Defendant breached its duties by, among other things:

a. Failing to exercise reasonable care in obtaining, retaining securing, safeguarding, deleting, and protecting the Personal Information in its possession;

b. Failing to protect the Personal Information in its possession by using reasonable and adequate security procedures and systems;

c. Failing to adequately and properly audit, test, and train its employees to avoid phishing emails;

d. Failing to use adequate email security systems, including industry standard SPAM filters, DMARC enforcement, and/or Sender Policy Framework enforcement to protect against phishing emails;

e. Failing to adequately and properly audit, test, and train its employees regarding how to properly and securely transmit and store Personal Information;

f. Failing to adequately train its employees to not store Personal Information longer than absolutely necessary for the specific purpose that it was sent or received;

g. Failing to consistently enforce security policies aimed at protecting Plaintiffs' and the Class's Personal Information;

h. Failing to implement processes to quickly detect data breaches, security incidents, or intrusions;

i. Failing to promptly notify Plaintiffs and Class members of the Data Breach that affected their Personal Information.

173. Defendant's willful failure to abide by these duties was wrongful, reckless, and grossly negligent in light of the foreseeable risks and known threats.

174. As a proximate and foreseeable result of Defendant's grossly negligent conduct, Plaintiffs and the Class have suffered damages and are at imminent risk of additional harms and damages (as alleged above).

175. Through Defendant's acts and omissions described herein, including but not limited to Defendant's failure to protect the Personal Information of Plaintiffs and Class members from being stolen and misused, Defendant unlawfully breached its duty to use reasonable care to adequately protect and secure the Personal Information of Plaintiffs and Class members while it was within Defendant's possession and control.

176. Further, through its failure to provide timely and clear notification of the Data Breach to Plaintiffs and Class members, Defendant prevented Plaintiffs and Class members from taking meaningful, proactive steps toward securing their Personal Information and mitigating damages.

177. As a result of the Data Breach, Plaintiffs and Class members have spent time, effort, and money to mitigate the actual and potential impact of the Data Breach on their lives, including but not limited to, responding to fraudulent activity, closely monitoring bank account activity, and examining credit reports and statements sent from providers and their insurance companies.

178. Defendant's wrongful actions, inactions, and omissions constituted (and continue to constitute) common law negligence.

179. The damages Plaintiffs and the Class have suffered (as alleged above) and will suffer were and are the direct and proximate result of Defendant's grossly negligent conduct.

180. In addition to its duties under common law, Defendant had additional duties imposed by statute and regulations, including the duties under the FTC Act. The harms which occurred as a result of Defendant's failure to observe these duties, including the loss of privacy, lost time and expense, and significant risk of identity theft are the types of harm that these statutes and regulations intended to prevent.

181. Defendant violated these statutes when it engaged in the actions and omissions alleged herein, and Plaintiffs' and Class members' injuries were a direct and proximate result of Defendant's violations of these statutes. Plaintiffs therefore are entitled to the evidentiary presumptions for negligence *per se*.

182. Pursuant to the FTC Act, 15 U.S.C. § 45(a), Defendant owed a duty to Plaintiffs and the Class to provide fair and adequate computer systems and data security to safeguard the Personal Information of Plaintiffs and the Class.

183. The FTC Act prohibits "unfair practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendant, of failing to use reasonable measures to protect Personal Information. The FTC publications and orders described above also formed part of the basis of Defendant's duty in this regard.

184. Defendant gathered and stored the Personal Information of Plaintiffs and the Class as part of its business, which affect commerce.

185. Defendant violated the FTC Act by failing to use reasonable measures to protect the Personal Information of Plaintiffs and the Class and by not complying with applicable industry standards, as described herein.

186. Defendant breached its duties to Plaintiffs and the Class under the FTC Act by failing to provide fair, reasonable, or adequate computer systems and/or data security practices to safeguard Plaintiffs' and Class members' Personal Information, and by failing to provide prompt and specific notice without reasonable delay.

187. Plaintiffs and the Class are within the class of persons that the FTC Act was intended to protect.

188. The harm that occurred as a result of the Data Breach is the type of harm the FTC Act was intended to guard against.

189. Defendant breached its duties to Plaintiffs and the Class under these laws by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiffs' and the Class's Personal Information.

190. Defendant breached its duties to Plaintiffs and the Class by unreasonably delaying and failing to provide notice of the Data Breach expeditiously and/or as soon as practicable to Plaintiffs and the Class.

191. As a direct and proximate result of Defendant's negligence, Plaintiffs and the Class have suffered, and continue to suffer, damages arising from the Data Breach, as alleged above.

192. The injury and harm that Plaintiffs and Class members suffered (as alleged above) was the direct and proximate result of Defendant's negligence.

193. Plaintiffs and the Class have suffered injury and are entitled to actual and punitive damages in amounts to be proven at trial.

COUNT TWO

BREACH OF IMPLIED CONTRACT

194. Plaintiffs incorporate by reference all allegations of the preceding paragraphs as though fully set forth herein.

195. Plaintiffs and Class Members were required to provide Defendant with their Personal Information in order to receive employment services and/or laundry services, tire inflation services, and/vacuum services.

196. When Plaintiffs and Class Members provided their Personal Information to Defendant when seeking these services, they entered into implied contracts in which Defendant agreed to comply with its statutory and common law duties to protect their Personal Information and to timely notify them in the event of a Data Breach.

197. Based on Defendant's representations, legal obligations, and acceptance of Plaintiffs' and the Class Members' Personal Information, Defendant had an implied duty to safeguard their Personal Information through the use of reasonable industry standards. This implied duty was reinforced by Defendant's representations in its Privacy Policy, which provides, *inter alia*: "We implement commercially reasonable technical, administrative, and organizational measures to protect Personal Information both online and offline from loss, misuse, and unauthorized access, disclosure, alteration, or destruction."[51]

198. Defendant breached the implied contracts by failing to safeguard Plaintiffs' and Class Members' Personal Information and failing to provide them with timely and accurate notice of the Data Breach. Indeed, it took Defendant *months* to warn Plaintiffs and Class Member of their imminent risk of identity theft. Defendant also failed to notify Plaintiffs and the Class

[51] https://www.cscsw.com/privacy-policy/.

Members whether or not their driver's license numbers were compromised, leaving Plaintiffs and Class Members unsure as to the extent of the information that was compromised.

199. As a direct and proximate result of Defendant's breach of implied contract, Plaintiffs and the Class Members have suffered damages, including foreseeable consequential damages that Defendant knew about when it requested Plaintiffs' and the Class Members' Personal Information.

COUNT THREE

UNJUST ENRICHEMNT

200. Plaintiffs incorporate by reference all allegations of the preceding paragraphs as though fully set forth herein.

201. Plaintiffs and the Class bring this claim in the alternative to all other claims and remedies at law.

202. Defendant collected, maintained, and stored the Personal Information of Plaintiffs and Class members as part its business operations and to gain profits. As such, Defendant had direct knowledge of the monetary benefits conferred upon it.

203. Defendant, by way of its affirmative actions and omissions, including its knowing violations of its implied contracts, knowingly and deliberately enriched itself by saving the costs it reasonably and contractually should have expended on reasonable data privacy and security measures to secure Plaintiffs' and Class members' Personal Information.

204. Instead of providing a reasonable level of security, training, and protocols that would have prevented the Data Breach, as described above and as is common industry practice among companies entrusted with similar Personal Information, Defendant, upon information and belief, instead consciously and opportunistically calculated to increase its own profits at the expense of Plaintiffs and Class members.

205. Defendant failed to implement—or adequately implement—data security practices, procedures, and programs to secure sensitive Personal Information, including without limitation those industry standard data security practices, procedures, and programs discussed herein.

206. As a direct and proximate result of Defendant's decision to profit rather than provide adequate data security, Plaintiffs and Class members suffered and continue to suffer actual damages, including (i) the amount of the savings and costs Defendant reasonably and contractually should have expended on data security measures to secure Plaintiffs' Personal Information, (ii) time and expenses mitigating harms, (iii) diminished value of Personal Information, (iv) loss of privacy, (v) harms as a result of identity theft; and (vi) an increased risk of future identity theft.

207. Defendant, upon information and belief, has therefore engaged in opportunistic and unethical conduct by profiting from conduct that it knew would create a significant and highly likely risk of substantial and certainly impending harm to Plaintiffs and the Class in direct violation of Plaintiffs' and Class members' interests. As such, it would be inequitable, unconscionable, and unlawful to permit Defendant to retain the benefits it derived as a consequence of its wrongful conduct.

208. Accordingly, Plaintiffs and the Class are entitled to relief in the form of restitution and disgorgement of all ill-gotten gains, which should be put into a common fund to be distributed to Plaintiffs and the Class.

VII. PRAYER FOR RELIEF

WHEREFORE, Plaintiffs and the Class pray for judgment against Defendant as follows:

a. An order certifying this action as a class action under Fed. R. Civ. P. 23, defining the Class as requested herein, appointing the undersigned as Class counsel, and finding that Plaintiffs is a proper representative of the Class requested herein;

b. A judgment in favor of Plaintiffs and the Class awarding them appropriate monetary relief, including actual damages, restitution, attorney fees, expenses, costs, and such other and further relief as is just and proper.

c. An order providing injunctive and other equitable relief as necessary to protect the interests of the Class and the general public as requested herein, including, but not limited to:

i. 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;

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

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

iv. Ordering that Defendant segment customer 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;

v. Ordering that Defendant cease transmitting Personal Information via unencrypted email;

vi. Ordering that Defendant cease storing Personal Information in email accounts;

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

viii. Ordering that Defendant conduct regular database scanning and securing checks;

ix. 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

x. Ordering Defendant to meaningfully educate its current, former, and prospective employees and subcontractors about the threats faced as a result of the loss of financial and personal information to third parties, as well as the steps they must take to protect against such occurrences;

d. An order requiring Defendant to pay the costs involved in notifying the Class members about the judgment and administering the claims process;

e. A judgment in favor of Plaintiffs and the Class awarding them pre-judgment and post-judgment interest, reasonable attorneys' fees, costs and expenses as allowable by law; and

f. An award of such other and further relief as this Court may deem just and proper.

VIII. DEMAND FOR JURY TRIAL

Plaintiffs demand a trial by jury on all issues so triable.

DATED: November 22, 2024

/s/ A. Brooke Murphy

A. Brooke Murphy
(admitted *pro hac vice*)
MURPHY LAW FIRM
4116 Will Rogers Pkwy, Suite 700
Oklahoma City, OK 73108
T: (405) 389-4989
E: abm@murphylegalfirm.com

Vicky J. Maniatis, Esq.
David K. Lietz
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN PLLC
100 Garden City Plaza, Suite 500
Garden City, New York 11530
Phone: (212) 594-5300
vmaniatis@milberg.com
dlietz@milberg.com

Scott Edward Cole
COLE & VAN NOTE
555 12th Street, Suite 2100
Oakland, California 94607
Telephone: (510) 891-9800
Facsimile: (510) 891-7030
sec@colevannote.com

Counsel for Plaintiffs and the Proposed Class

CERTIFICATE OF SERVICE

I hereby certify that this document filed through the CM/ECF system will be sent electronically to the registered participants as identified on the Notice of Electronic Filing and paper copies will be sent to those indicated as non-registered participants on November 22, 2024.

/s/ A. Brooke Murphy
A. Brooke Murphy