Exhibit A

IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA
Newport News Division

IN RE R&B CORPORATION OF VIRGINIA d/b/a CREDIT CONTROL CORPORATION, DATA SECURITY BREACH LITIGATION	**CASE NO. 4:23-cv-00066-JKW-RJK** **AMENDED CONSOLIDATED CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

Plaintiffs Veronica Huamani, Christina Pearson, Shiree Lackland, Stephanie Moxley, Douglas Monson, Merrette Blake, Jason Powers, Michele Van Moppes, and ("Plaintiffs"), individually and on behalf of all others similarly situated ("Class Members"), bring this Amended Consolidated Class Action Complaint against R&B Corporation of Virginia d/b/a Credit Control Corporation ("R&B" or "Defendant") and allege, upon personal knowledge as to their own actions and their counsel's investigations, and upon information and belief as to all other matters, as follows:

NATURE OF ACTION

1. Plaintiffs bring this class action against R&B for its failure to secure and safeguard the personally identifying information ("PII") of over two-hundred thousand people, including names, addresses, financial account information and, critically, Social Security numbers.

2. R&B is a debt collection agency that specializes in "in healthcare, utility, and commercial collections."[1] On its computer network, R&B holds and stores certain highly sensitive

[1] https://creditcontrol.net/about-us/ (last visited Aug. 17, 2023).

personally identifiable information ("PII" or "Private Information") of the Plaintiffs and the putative Class Members, who are customers of R&B's business partners, i.e., individuals who provided their highly sensitive and private information in exchange for employment, utilities and/or other business services.

3. According to the Notice of Data Breach Letter that R&B sent to Plaintiffs and Class members, R&B first became aware of the "unusual activity" on its computer network on March 7, 2023.[2]

4. R&B finally began notifying the victims on or about May 15, 2023, over 2 months after the data breach occurred, stating that their PII had been stolen.[3]

5. R&B's notice explained that "certain files were copied from [its] network as part of a cyber incident that occurred between March 2, 2023 and March 7, 2023" and that its investigation "undertook a thorough review of the files in order to identify what specific information was present in the files..."[4]

6. Based upon R&B's website notification and its notice letter, the Private Information compromised in the Data Breach was intentionally accessed and removed, also called exfiltrated, by the cyber-criminals who perpetrated this attack and remains in the hands of those cybercriminals.

7. As noted above, the Data Breach was a direct result of R&B's failure to implement adequate and reasonable cyber-security procedures and protocols necessary to protect Plaintiffs and Class Members' Private Information.

---

[2] *See* https://apps.web.maine.gov/online/aeviewer/ME/40/a5270b26-3247-48fd-ab4a-f68eb29248df.shtml (last visited: August 14, 2023).

[3] *Id*.

[4] *Id*.

8. Plaintiffs bring this class action lawsuit on behalf of those similarly situated to address R&B's inadequate safeguarding of Class Members' Private Information that they collected and maintained, and for failing to provide timely and adequate notice to Plaintiffs and other Class Members that their information had been subject to the unauthorized access of an unknown third party and precisely what specific type of information was accessed.

9. R&B maintained the Private Information in a reckless manner. In particular, the Private Information was maintained on Defendant's computer network in a condition vulnerable to cyberattacks. The mechanism of the cyberattack and potential for improper disclosure of Plaintiffs' and Class Members' Private Information was a known risk to R&B. Thus, Defendant was on notice that failing to take steps necessary to secure the Private Information from those risks left that property in a dangerous condition.

10. R&B disregarded the privacy and property rights of Plaintiffs and Class Members by, inter alia, intentionally, willfully, recklessly, or negligently failing to take adequate and reasonable measures to ensure its data systems were protected against unauthorized intrusions; failing to disclose that it did not have adequately robust computer systems and security practices to safeguard Class Members' Private Information; failing to take standard and reasonably available steps to prevent the Data Breach; and failing to provide Plaintiffs and Class Members prompt and complete notice of the Data Breach.

11. In addition, R&B and its employees failed to properly monitor the computer network and systems that housed the Private Information. Had R&B properly monitored its computers, it would have discovered the intrusion sooner, and potentially been able to mitigate the injuries to Plaintiffs and the Class.

12. Plaintiffs' and Class Members' identities are now at substantial and imminent risk because of Defendant's negligent conduct since the Private Information that Defendant collected and maintained (including Social Security numbers) is now in the hands of data thieves.

13. Armed with the Private Information accessed in the Data Breach, data thieves can commit a variety of crimes including, e.g., opening new financial accounts in Class Members' names, taking out loans in Class Members' names, using Class Members' information to obtain government benefits, filing fraudulent tax returns using Class Members' information, filing false medical claims using Class Members' information, obtaining driver's licenses in Class Members' names but with another person's photograph, and giving false information to police during an arrest.

14. As a result of the Data Breach, Plaintiffs and Class Members have been exposed to a heightened and imminent risk of fraud and identity theft. Plaintiffs and Class Members must now and in the future closely monitor their financial accounts to guard against identity theft.

15. Plaintiffs and Class Members may also incur out of pocket costs for, e.g., purchasing credit monitoring services, credit freezes, credit reports, or other protective measures to deter and detect identity theft.

16. Through this Complaint, Plaintiffs seek to remedy these harms on behalf of themselves and all similarly situated individuals whose Private Information was accessed during the Data Breach.

17. Accordingly, Plaintiffs bring this action against Defendant for negligence, negligence *per se* based upon violations of Section 5 of the FTC Act and the Virginia Personal Information Breach Notification Act, breach of implied contract, breach of contracts to which Plaintiffs and class members were intended third party beneficiaries, unjust enrichment, violations

of the Virginia Consumer Protection Act, violations of the North Carolina Unfair and Deceptive Trade Practices Act, violations of the West Virginia Consumer Credit Protection Act, and declaratory relief, seeking redress for Defendant's unlawful conduct.

18. Plaintiffs seek remedies including, but not limited to, compensatory damages, reimbursement of out-of-pocket costs, and injunctive relief including improvements to Defendant's data security systems, future annual audits, and adequate, long term credit monitoring services funded by Defendant, and declaratory relief.

THE PARTIES

19. Plaintiff Veronica Huamani is an adult, who at all relevant times, was a resident and citizen of the Commonwealth of Virginia. Plaintiff Huamani received a notice from Defendant informing her that her Private Information had been compromised during the Data Breach.

20. Plaintiff Christina Pearson is an adult, who at all relevant times, was a resident and citizen of the Commonwealth of Virginia. Plaintiff Pearson received a notice from Defendant informing her that her PII and PHI had been compromised during the Data Breach.

21. Plaintiff Shiree Lackland is an adult, who at all relevant times, was a resident and citizen of the Commonwealth of Virginia. Plaintiff Lackland received a notice from Defendant informing her that her PII and PHI had been compromised during the Data Breach.

22. Plaintiff Stephanie Moxley is an adult, who at all relevant times, was a resident and citizen of the state of West Virginia. Plaintiff Lackland received a notice from Defendant informing her that her PII and PHI had been compromised during the Data Breach.

23. Plaintiff Douglas Monson is an adult, who at all relevant times, was a resident and citizen of the State of Texas. Plaintiff Monson received a notice from Defendant informing him that his Private Information had been compromised during the Data Breach.

24. Plaintiff Merrette Blake is an adult, who at all relevant times, was a resident and citizen of the Commonwealth of Virginia. Plaintiff Blake received a notice from Defendant informing him that his Private Information had been compromised during the Data Breach.

25. Plaintiff Jason Powers is an adult, who at all relevant times, was a resident and citizen of the state of North Carolina. Plaintiff Powers received a notice from Defendant informing him that his Private Information had been compromised during the Data Breach.

26. Plaintiff Michele Van Moppes is an adult, who at all relevant times, was a resident and citizen of the Commonwealth of Virginia. Plaintiff Huamani received a notice from Defendant informing her that her Private Information had been compromised during the Data Breach.

27. Defendant R & B Corporation of Virginia d/b/a Credit Control Corporation is a Virginia stock corporation organized and headquartered in Newport News, Virginia. Defendant's principal place of business is located at 11821 Rock Landing Dr., Newport News, Virginia 23606.

JURISDICTION AND VENUE

28. This Court has subject matter jurisdiction over this action pursuant to the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). The amount in controversy exceeds $5 million, exclusive of interest and costs. The number of class members exceeds 100, many of whom have different citizenship from Defendant, including certain Plaintiffs. Thus, minimal diversity exists under 28 U.S.C. § 1332(d)(2)(A).

29. The Court has general personal jurisdiction over Defendant because, personally or through its agents, Defendant operates, conducts, engages in, or carries on a business or business venture in this State; it is registered with the Secretary of State as a stock corporation; it maintains its headquarters in Virginia; and committed tortious acts in Virginia.

30. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(a)(1) because Defendant is based in this District, and the acts and omissions giving rise to Plaintiff's claims occurred in and emanated from this District.

FACTUAL ALLEGATIONS

Background

31. Defendant claims it "provides superior collection services for clients, professional communications with consumers, and an energized working environment for employees."[5]

32. Defendant has "over 60 years of experience, [and] Credit Control Corporation (CCC) is the partner of choice specializing in healthcare, utility, and commercial collections."[6]

33. Additionally, Defendant has pledged to "remain compliant" with various privacy laws, including the "FDCPA, FCRA, HIPAA, PCI, FTC, UDAAP, and GLBA regulations pertaining to debt collection operations and to educate/train and monitor our employees accordingly. Our success is evidenced by the hundreds of healthcare clients who have made Defendant the vendor of choice for their business needs."[7]

34. Defendant, in the regular course of its business, collects and maintains the PII of employees (on behalf of its customers) as a requirement of its business practices.

35. The customers of Defendant provide their employees' and clients' PII with the mutual understanding that this highly sensitive private information is confidential and must be properly safeguarded from misuse and theft.

36. In addition, as a debt collection agency for medical providers, Defendant collects and stores highly sensitive medical and health information ("PHI") about individuals on its

[5] https://creditcontrol.net/about-us/ (last accessed June 1, 2023).

[6] *Id*.

[7] *Id*.

computer systems. This PHI requires Defendant to adhere to the laws, rules and regulations of HIPAA. Defendant is aware of and publicly acknowledges its obligations on its website.[8]

37. Defendant promises, among other things, that in order "[t]o provide even more assurance, an independent firm conducts an annual SOC audit to attest that Defendant's internal controls are suitably designed and operating effectively. With these safeguards and a $5M cyber-liability insurance policy, our clients can take comfort that customers' protected information (PHI) is safe on our network."[9]

38. In the course of collecting Private Information from consumers, including Plaintiffs and Class Members, Defendant promised to provide confidentiality and adequate security for Private Information through its applicable Privacy Policy and in compliance with statutory privacy requirements applicable to its industry. Defendant is aware of and had obligations created by HIPAA FTCA, contract, industry standards, and common law to keep Plaintiffs' and Class Members' Private Information confidential and to protect it from unauthorized access and disclosure.

39. Defendant claims that "the privacy of all users of www.creditcontrol.net is of the highest priority." Plaintiffs and the Class Members, as consumers, relied on the promises and duties of CCC to keep their sensitive PII confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information.

40. Consumers, in general, demand that businesses that require highly sensitive PII will provide security to safeguard their PII, especially when Social Security numbers and private health

[8] *Id*.

[9] *Id*.

information are involved.

41. In the course of its business, R&B's customers provided it with the highly sensitive PII of Plaintiffs and Class Members.

42. R&B had a duty to adopt reasonable measures to protect Plaintiffs' and Class Members' PII and PHI from unauthorized disclosure to third parties.

43. Defendant agreed to and undertook legal duties to maintain the PII of Plaintiffs and Class Members safely, confidentially, and in compliance with all applicable laws.

44. Plaintiffs and Class Members have taken reasonable steps to maintain the confidentiality of their PII.

45. Plaintiffs and Class Members relied on Defendant to keep their PII confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosure of this Private Information.

46. Upon information and belief, Defendant made promises and representations to its customers, including Plaintiffs and Class Members, that the PII collected from them and entrusted would be kept safe, confidential, that the privacy of that information would be maintained, and that Defendant would delete any sensitive information after it was no longer required to maintain it.

47. Plaintiffs and Class Members directly or indirectly entrusted Defendant with sensitive and confidential information, including their PII which includes information that is static, meaning it does not change, and can be used to commit myriad financial crimes.

48. Defendant had a duty to adopt reasonable measures to protect the PII of Plaintiffs and Class Members from involuntary disclosure to third parties.

49. Defendant derived a substantial economic benefit from collecting Plaintiff's and

Class Members' PII. Without the required submission of PII, Defendant could not perform the services they provide.

50. By obtaining, collecting, using, and deriving a benefit from Plaintiff's and Class Members' PII, Defendant assumed legal and equitable duties and knew or should have known that it was responsible to protect Plaintiff's and Class Members' PII from unauthorized disclosure, and that such an attempt to obtain said information was foreseeable.

The Data Breach

51. According to its Notice Letters, on March 7, 2023, CCC became aware of "unusual activity involving certain systems within CCC's network." After an unspecified amount of time, between the date they "became aware" and sent the notice letters, its investigation determined that an unauthorized actor accessed the CCC network and exfiltrated the data.[10]

52. The letter specifies that that unauthorized actor accessed CCC's network sometime between March 2, 2023 and March 7, 2023, and was able to extract certain data from the network during that time period.

53. Defendant reported to State Attorneys General that some of the information breached contained names and Social Security numbers.[11]

54. Therefore, Plaintiffs' and Class Members' PII was in the hands of cybercriminals for over 2 months before Plaintiffs and Class Members were notified of CCC's Data Breach. Time is of the essence when trying to protect against identity theft after a data breach, so early notification is critical.

---

[10] https://creditcontrol.net/notice-of-data-incident/ (Last accessed May 30, 2023).

[11] *See, e.g.* https://apps.web.maine.gov/online/aeviewer/ME/40/6a11760a-5f54-4fa7-b222-f74eed5cf516.shtml; https://oag.my.site.com/datasecuritybreachreport/apex/DataSecurityReportsPage (Last accessed May 30, 2023)

55. Defendant admits that the files exfiltrated from CCC contained at least the following information of Plaintiffs and Class Members: "name, address, Social Security number, and information relating to the individual's account(s) with our business partner(s) such as account number, account balance, and date of service."[12]

56. Plaintiffs' Private Information was accessed and stolen in the Data Breach. Plaintiffs reasonably believe their stolen Private Information is currently available for sale on the Dark Web because that is the modus operandi of cybercriminals who target businesses that collect highly sensitive Private Information.

57. As a result of the Data Breach, Defendant now encourages Class Members to enroll in credit monitoring, fraud consultation, and identity theft restoration services, a tacit admission of the imminent risk of identity theft faced by Plaintiffs and Class members.

58. That Defendant is encouraging Plaintiffs and Class Members to enroll in credit monitoring and identity theft restoration services is an acknowledgment that the impacted consumers are subject to a substantial and imminent threat of fraud and identity theft.

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

60. Defendant could have prevented or mitigated this Data Breach by, among other things, better securing its network, properly encrypting its data, or better selecting supervising its information technology partners. Defendant's negligence in safeguarding Plaintiff's and Class Members' PII and PHI was exacerbated by repeated warnings and alerts directed to protecting and securing sensitive data, as evidenced by the trending data breach attacks in recent years. In 2022,

[12] https://creditcontrol.net/notice-of-data-incident/

the damages from identity theft was projected to reach $8 trillion dollars.[13]

Plaintiff Merrette Blake's Experience

61. Plaintiff Blake greatly values his privacy and is very careful with his Private Information.

62. Plaintiff Blake stores any documents containing Private Information in a safe and secure location or destroys such documents when they are no longer needed.

63. Plaintiff Blake has never knowingly transmitted unencrypted sensitive Private Information over the internet or any other unsecured source.

64. Plaintiff Blake diligently chooses unique usernames and passwords for his various online accounts.

65. When Plaintiff Blake does entrust a third-party with his Private Information, it is only because he understands such information will be reasonably safeguarded from foreseeable threats, and that he will be timely notified if his data is exposed.

66. Plaintiff Blake received a letter dated May 15, 2023 from Defendant notifying him of the Data Breach. The letter advised that unauthorized third parties accessed Defendant's network. The letter further advised that Plaintiff Blake's Private Information—including his name, Social Security number, date of service, medical provider, patient account balance, and patient account number—was identified as having been "copied from [Defendant's] network."

67. Recognizing the present, immediate, and substantially increased risk of harm Plaintiff Blake faces, the letter offered Plaintiff Blake a one-year subscription to credit monitoring services. The letter further instructed Plaintiff Blake to "remain vigilant against incidents of identity theft and fraud by reviewing your account statements and monitoring your free credit

[13] https://www.juniperresearch.com/press/cybercrime-to-cost-global-business-over-8-trn.

reports for suspicious activity."

68. As a result of the Data Breach, Plaintiff 8 has spent approximately 8-9 hours researching the Data Breach, verifying the legitimacy of the notice letter, signing up for the credit monitoring service, reviewing his bank accounts, monitoring his credit report, changing his passwords and payment account numbers and other necessary mitigation efforts. This is valuable time Plaintiff Blake spent at Defendant's direction and that he otherwise would have spent on other activities, including but not limited to work and/or recreation.

69. Plaintiff Blake incurred out-of-pocket expenses relating to postage from mailing his credit card companies for detailed reports.

70. Plaintiff Blake incurred out-of-pocket expenses from the purchase of credit monitoring service Identity IQ in the amount of $39.99 per month since the Data Breach. Given Defendant's Data Breach, Plaintiff Blake did not feel comfortable using R&B's free credit monitoring service.

71. The Data Breach also caused Plaintiff Blake to suffer a loss of privacy.

72. As a result of the Data Breach, Plaintiff Blake will face a substantial risk of imminent harm for the rest of his life.

73. Plaintiff Blake anticipates spending additional considerable time and money on an ongoing basis to try to mitigate and address the present and impending injuries caused by the Data Breach.

74. The substantial risk of harm and loss of privacy from the Data Breach has caused Plaintiff Blake to suffer fear, anxiety, annoyance, inconvenience, and nuisance.

75. The Data Breach caused Plaintiff Blake to suffer a diminution in the value of his Private Information.

76. Plaintiff Blake has a continuing interest in ensuring that his Private Information, which upon information and belief, remains in Defendant's possession, is protected and safeguarded from future breaches.

77. As a result of the Data Breach, Plaintiff has also suffered injury directly and proximately caused by the Data Breach, including: (a) theft of Plaintiff's valuable Private Information; (b) the imminent and certain impending injury flowing from fraud and identity theft posed by Plaintiff's Private Information being placed in the hands of cyber criminals; (c) damages to and diminution in value of Plaintiff's Private 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 he made with Defendant by overpaying for services that were intended to be accompanied by adequate data security but were not; (e) loss of time and effort that Plaintiff Blake has had to expend in an attempt to ameliorate, mitigate, and address the consequences of the Data Breach, with such steps being taken at the direction of Defendant; and (f) continued risk to Plaintiff's Private 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 Private Information that was entrusted to Defendant.

Plaintiff Shiree Lackland's Experience

78. Subsequent to the Data Breach, and in addition to the injuries alleged above, Plaintiff Lackland expended time taking the proactive step of freezing her credit card accounts after receiving CCC's notification letter.

79. Plaintiff Lackland has spent approximately 8 hours scouring her credit card accounts for fraudulent activity, including taking steps to freeze her accounts, as a result of the Data Breach. The time spent dealing with these incidents resulting from the Data Breach is time

Plaintiff Lackland otherwise would have spent on other activities, such as work and/or recreation. Moreover, the time Plaintiff lost was spent at Defendant's direction. Indeed, in the notice letter Plaintiff Lackland received, Defendant directed Plaintiff to spend time mitigating her losses by reviewing her accounts and credit reports for unauthorized activity.

80. Plaintiff Lackland plans on taking additional time-consuming, necessary steps to help mitigate the harm caused by the Data Breach, including continually reviewing her accounts for any unauthorized activity.

81. As a result of the Data Breach, Plaintiff Lackland has also suffered injury directly and proximately caused by the Data Breach, including: (a) theft of Plaintiff's valuable Private Information; (b) the imminent and certain impending injury flowing from fraud and identity theft posed by Plaintiff's Private Information being placed in the hands of cyber criminals; (c) damages to and diminution in value of Plaintiff's Private 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 he made with Defendant by overpaying for services that were intended to be accompanied by adequate data security but were not; (e) loss of time and effort that Plaintiff Lackland has had to expend in an attempt to ameliorate, mitigate, and address the consequences of the Data Breach, with such steps being taken at the direction of Defendant; and (f) continued risk to Plaintiff's Private 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 Private Information that was entrusted to Defendant.

Plaintiff Veronica Huamani's Experience

82. Subsequent to the Data Breach, and in addition to the injuries alleged above, Plaintiff Huamani experienced actual fraud. An unknown individual attempted to open an account

with Bank of America in her name in May 2023. This required Plaintiff Huamani to spend time and take additional steps to work with her bank to close the fraudulent account. Plaintiff Huamani also signed up for credit monitoring through CCC following the Data Breach to monitor her accounts for additional fraudulent activity.

83. Plaintiff Huamani has spent several hours addressing the fraudulent activity and otherwise as a result of the Data Breach. The time spent dealing with these incidents resulting from the Data Breach is time Plaintiff Huamani otherwise would have spent on other activities, such as work and/or recreation. Moreover, the time Plaintiff Huamani lost was spent at Defendant's direction. Indeed, in the notice letter Plaintiff Huamani received, Defendant directed Plaintiff Huamani to spend time mitigating her losses by reviewing her accounts and credit reports for unauthorized activity.

84. Plaintiff Huamani plans on taking additional time-consuming, necessary steps to help mitigate the harm caused by the Data Breach, including continually reviewing her accounts for any unauthorized activity.

85. As a result of the Data Breach, Plaintiff Huamani has also suffered injury directly and proximately caused by the Data Breach, including: (a) theft of Plaintiff's valuable Private Information; (b) the imminent and certain impending injury flowing from fraud and identity theft posed by Plaintiff's Private Information being placed in the hands of cyber criminals; (c) damages to and diminution in value of Plaintiff's Private 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 he made with Defendant by overpaying for services that were intended to be accompanied by adequate data security but were not; (e) loss of time and effort that Plaintiff Huamani has had to expend in an attempt to ameliorate, mitigate, and address the consequences of

the Data Breach, with such steps being taken at the direction of Defendant; and (f) continued risk to Plaintiff's Private 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 Private Information that was entrusted to Defendant.

Plaintiff Michele Van Moppes's Experience

86. Subsequent to the Data Breach, and in addition to the injuries alleged above, Plaintiff Van Moppes experienced fraudulent activity with her accounts. Specifically, she received a credit application update from Walmart about the status of an application that she never filled out. She had to contact Walmart to explain that she did not create the account and have the new application rejected. She additionally has been receiving suspicious emails requesting her contact information to pick up a package which she did not order. She has ignored these requests as she believes they are fraudulent.

87. Plaintiff Van Moppes has spent approximately 15-20 hours scouring her credit card accounts for fraudulent activity, communicating with Walmart about the fraudulent credit application, and otherwise monitoring her accounts as a result of the Data Breach. The time spent dealing with these incidents resulting from the Data Breach is time Plaintiff Van Moppes otherwise would have spent on other activities, such as work and/or recreation. Moreover, the time Plaintiff lost was spent at Defendant's direction. Indeed, in the notice letter Plaintiff Van Moppes received, Defendant directed Plaintiff to spend time mitigating her losses by reviewing her accounts and credit reports for unauthorized activity.

88. Plaintiff Van Moppes plans on taking additional time-consuming, necessary steps to help mitigate the harm caused by the Data Breach, including continually reviewing her accounts for any unauthorized activity.

89. As a result of the Data Breach, Plaintiff Van Moppes has also suffered injury directly and proximately caused by the Data Breach, including: (a) theft of Plaintiff's valuable Private Information; (b) the imminent and certain impending injury flowing from fraud and identity theft posed by Plaintiff's Private Information being placed in the hands of cyber criminals; (c) damages to and diminution in value of Plaintiff's Private 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 he made with Defendant by overpaying for services that were intended to be accompanied by adequate data security but were not; (e) loss of time and effort that Plaintiff Van Moppes has had to expend in an attempt to ameliorate, mitigate, and address the consequences of the Data Breach, with such steps being taken at the direction of Defendant; and (f) continued risk to Plaintiff's Private 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 Private Information that was entrusted to Defendant.

Plaintiff Christina Pearson's Experience

90. Subsequent to the Data Breach, and in addition to the injuries alleged above, Plaintiff Pearson experienced actual fraudulent activity on her Venmo account. Between the time period of May to June 2023, Venmo called Plaintiff Pearson repeatedly, upward of 40 times, to verify that the phone number was linked to the account. This was very suspicious to Plaintiff Pearson as she did not make any changes to her Venmo account. She was forced to close her Venmo account as a result of this suspicious activity.

91. Plaintiff Pearson has spent approximately two hours going through her credit reports to monitor for suspicious activity and otherwise as a result of the Data Breach. She spent

an additional 4 to 5 hours on the phone to address the suspicious Venmo activity. The time spent dealing with these incidents resulting from the Data Breach is time Plaintiff Pearson otherwise would have spent on other activities, such as work and/or recreation. Moreover, the time Plaintiff Pearson lost was spent at Defendant's direction. Indeed, in the notice letter Plaintiff Pearson received, Defendant directed Plaintiff Pearson to spend time mitigating her losses by reviewing her accounts and credit reports for unauthorized activity.

92. Plaintiff Pearson plans on taking additional time-consuming, necessary steps to help mitigate the harm caused by the Data Breach, including continually reviewing her accounts for any unauthorized activity.

93. As a result of the Data Breach, Plaintiff Pearson has also suffered injury directly and proximately caused by the Data Breach, including: (a) theft of Plaintiff's valuable Private Information; (b) the imminent and certain impending injury flowing from fraud and identity theft posed by Plaintiff's Private Information being placed in the hands of cyber criminals; (c) damages to and diminution in value of Plaintiff's Private 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 he made with Defendant by overpaying for services that were intended to be accompanied by adequate data security but were not; (e) loss of time and effort that Plaintiff Pearson has had to expend in an attempt to ameliorate, mitigate, and address the consequences of the Data Breach, with such steps being taken at the direction of Defendant; and (f) continued risk to Plaintiff's Private 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 Private Information that was entrusted to Defendant.

Plaintiff Douglas Monson's Experience

94. Subsequent to the Data Breach, and in addition to the injuries alleged above, Plaintiff Monson experienced actual fraudulent attempts associated with his bank account at Navy Federal Bank. Specifically, in or around June and July 2023, Plaintiff Monson experienced suspicious bank account logins that prompted the bank to contact him to verify his account activity. Plaintiff Monson also experienced suspicious Facebook login attempts.

95. Plaintiff Monson has spent approximately six hours addressing the fraudulent activity associated with his bank account, including calling Navy Federal Bank, changing his bank account logins, adding "red flag monitoring" to his account and to otherwise monitor for suspicious activity. Plaintiff Monson spent an additional 8 hours monitoring his other accounts and changing all other login information for his online accounts per the recommendation of Navy Federal Bank. The time spent dealing with these incidents resulting from the Data Breach is time Plaintiff Monson otherwise would have spent on other activities, such as work and/or recreation. Moreover, the time Plaintiff Monson lost was spent at Defendant's direction. Indeed, in the notice letter Plaintiff Monson received, Defendant directed Plaintiff Monson to spend time mitigating his losses by reviewing his accounts and credit reports for unauthorized activity.

96. Plaintiff Monson plans on taking additional time-consuming, necessary steps to help mitigate the harm caused by the Data Breach, including continually reviewing his accounts for any unauthorized activity.

97. As a result of the Data Breach, Plaintiff Monson has also suffered injury directly and proximately caused by the Data Breach, including: (a) theft of Plaintiff's valuable Private Information; (b) the imminent and certain impending injury flowing from fraud and identity theft posed by Plaintiff's Private Information being placed in the hands of cyber criminals; (c) damages

to and diminution in value of Plaintiff's Private 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 he made with Defendant by overpaying for services that were intended to be accompanied by adequate data security but were not; (e) loss of time and effort that Plaintiff Monson has had to expend in an attempt to ameliorate, mitigate, and address the consequences of the Data Breach, with such steps being taken at the direction of Defendant; and (f) continued risk to Plaintiff's Private 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 Private Information that was entrusted to Defendant.

Plaintiff Stephanie Moxley's Experience

98. Subsequent to the Data Breach, and in addition to the injuries alleged above, Plaintiff Moxley took proactive steps to monitor her accounts for suspicious activity as a result of the Data Breach.

99. Plaintiff Moxley has spent approximately three hours searching her financial accounts for suspicious activity and otherwise as a result of the Data Breach. The time spent dealing with these incidents resulting from the Data Breach is time Plaintiff Moxley otherwise would have spent on other activities, such as work and/or recreation. Moreover, the time Plaintiff Moxley lost was spent at Defendant's direction. Indeed, in the notice letter Plaintiff Moxley received, Defendant directed Plaintiff Moxley to spend time mitigating her losses by reviewing her accounts and credit reports for unauthorized activity.

100. Plaintiff Moxley plans on taking additional time-consuming, necessary steps to help mitigate the harm caused by the Data Breach, including continually reviewing her accounts for any unauthorized activity.

101. As a result of the Data Breach, Plaintiff Moxley has also suffered injury directly and proximately caused by the Data Breach, including: (a) theft of Plaintiff's valuable Private Information; (b) the imminent and certain impending injury flowing from fraud and identity theft posed by Plaintiff's Private Information being placed in the hands of cyber criminals; (c) damages to and diminution in value of Plaintiff's Private 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 he made with Defendant by overpaying for services that were intended to be accompanied by adequate data security but were not; (e) loss of time and effort that Plaintiff Moxley has had to expend in an attempt to ameliorate, mitigate, and address the consequences of the Data Breach, with such steps being taken at the direction of Defendant; and (f) continued risk to Plaintiff's Private 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 Private Information that was entrusted to Defendant.

Plaintiff Jason Powers' Experience

102. Plaintiff Jason Powers does not know how Defendant obtained his Private Information, and he had never heard of Defendant until he received the notice letter regarding the Data Breach in May 2023.

103. Plaintiff Powers is very careful about sharing his sensitive Private Information. Plaintiff Powers has never knowingly transmitted unencrypted sensitive Private Information over the internet or any other unsecured source.

104. Plaintiff Powers first learned of the Data Breach after receiving a data breach notification letter from R&B, dated May 15, 2023, notifying him that Defendant suffered a data breach two months earlier and that his Private Information had been improperly accessed and/or

obtained by unauthorized third parties while in possession of Defendant.

105. The data breach notification letter indicated that the Private Information involved in the Data Breach may have included Plaintiff Powers' full name, Social Security number, date of service, medical provider, patient account balance, and patient account number.

106. As a result of the Data Breach, Plaintiff Powers made reasonable efforts to mitigate the impact of the Data Breach after receiving the data breach notification letter, including but not limited to: contacting credit bureaus to place freezes on their accounts and monitoring their financial accounts for unauthorized activity, which may take years to discover and detect. Plaintiff Powers has spent significant time—at least four hours thus far—and will continue to spend valuable time for the remainder of his life, that he otherwise would have spent on other activities, including but not limited to work and/or recreation.

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

108. As a result of the Data Breach, Plaintiff Powers has also suffered emotional distress as a result of the release of his Private Information, which he believed would be protected from unauthorized access and disclosure, including anxiety about unauthorized parties viewing, selling, and/or using his Private Information for purposes of identity theft and fraud. Plaintiff Powers is very concerned about identity theft and fraud, as well as the consequences of such identity theft and fraud resulting from the Data Breach.

109. As a result of the Data Breach, Plaintiff Powers anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach.

Value of PII

110. The Federal Trade Commission ("FTC") defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority."[14] The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number."[15]

111. The PII of individuals remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials. For example, personal information can be sold at a price ranging from $40 to $200, and bank details have a price range of $50 to $200.[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 $900 to $4,500.[18]

---

[14] 17 C.F.R. § 248.201 (2013)

[15] *Id.*

[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-dark-web-how-much-it-costs/ (last accessed Mar. 25, 2023).

[17] *Here's How Much Your Personal Information Is Selling for on the Dark Web*, Experian, Dec. 6, 2017, *available at*: https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/ (last accessed Mar. 25, 2023).

[18] *In the Dark*, VPNOverview, 2019, *available at*: https://vpnoverview.com/privacy/

112. For example, Social Security numbers are among the worst kind of PII to have stolen because they may be put to a variety of fraudulent uses and are difficult for an individual to change. The Social Security Administration stresses that the loss of an individual's Social Security number, as experienced by Plaintiffs and some Class Members, 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.[19]

113. 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.

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

---

anonymous-browsing/in-the-dark/ (last accessed Mar. 25, 2023).

[19] Social Security Administration, *Identity Theft and Your Social Security Number, available at:* https://www.ssa.gov/pubs/EN-05-10064.pdf (last visited May 17, 2023).

[20] Bryan Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back,* NPR (Feb. 9, 2015), *available at:* https://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millions-worrying-about-identity-theft (last visited May 17, 2023).

115. 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.

116. 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 … [is] worth more than 10x on the black market."[21]

117. Moreover, there may be a time lag between when harm occurs versus when it is discovered, and also between when PII 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 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.[22]

118. At all relevant times, Defendant knew, or reasonably should have known, of the importance of safeguarding the PII of Plaintiffs and Class Members and the foreseeable consequences that would occur if Defendant's data security system was breached, including, specifically, the significant costs that would be imposed on Plaintiffs and Class Members as a result of a breach.

119. Plaintiffs and Class Members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. The Class is incurring and will

---

[21] 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 (last accessed Mar. 25, 2023).

[22] *Report to Congressional Requesters*, GAO, at 29 (June 2007), *available at:* https://www.gao.gov/assets/gao-07-737.pdf (last accessed Aug. 23, 2021).

continue to incur such damages in addition to any fraudulent use of their PII.

120. Defendant were, or should have been, fully aware of the unique type and the significant volume of data on Defendant's network and, thus, the significant number of individuals who would be harmed by the exposure of the compromised data.

121. The injuries to Plaintiffs and Class Members were directly and proximately caused by Defendant's failure to implement or maintain adequate data security measures for the PII of Plaintiffs and Class Members.

122. By 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 they were responsible for protecting Plaintiff's and Class Members' Private Information from unauthorized disclosure.

123. Plaintiffs and the Class Members have taken reasonable steps to maintain the confidentiality of their Private Information.

124. Plaintiffs and the Class Members relied on Defendant to implement and follow adequate data security policies and protocols, to keep their Private Information confidential and securely maintained, to use such Private Information solely for business and health care purposes, and to prevent the unauthorized disclosures of the Private Information.

The Data Breach was Foreseeable and Preventable

125. As explained by the Federal Bureau of Investigation, "[p]revention is the most effective defense against ransomware and it is critical to take precautions for protection."[23]

126. Defendant's data security obligations were particularly important given the

[23] *See* How to Protect Your Networks from RANSOMWARE, at 3, *available at* https://www.fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf/view (last accessed May 17, 2023).

substantial increase in cyberattacks and/or data breaches preceding the date of the breach at issue in this case.

127. In 2021, a record 1,862 data breaches occurred, resulting in approximately 293,927,708 sensitive records being exposed. [24] In 2022, there was a 41.5% increase in the number of victims impacted.[25] The 330 reported breaches in 2021 exposed nearly 30 million sensitive records (28,045,658), compared to only 306 breaches that exposed nearly 10 million sensitive records (9,700,238) in 2020.

128. Indeed, cyberattacks have become so notorious that the Federal Bureau of Investigation ("FBI") and U.S. Secret Service have issued a warning to potential targets, so they are aware of, and prepared for, a potential attack.[26]

129. In fact, according to the cybersecurity firm Mimecast, 90% of healthcare organizations experienced cyberattacks in the past year. [27]

130. Therefore, the increase in such attacks, and attendant risk of future attacks, was widely known to the public and to anyone in Defendant's industry, including Defendant.

131. To prevent and detect cyber-attacks Defendant could and should have implemented, as recommended by the United States Cybersecurity & Infrastructure Security Agency, the following measures:

---

[24] See *Identity Theft Resource Center's 2021 Annual Data Breach Report Sets New Record for Number of Compromises,* https://www.idtheftcenter.org/post/identity-theft-resource-center-2021-annual-data-breach-report-sets-new-record-for-number-of-compromises/?utm_source=press+release&utm_medium=website&utm_campaign=2022+Annual+Data+Breach+Report.

[25] *Identity Theft Resource Center's 2022 Annual Data Breach Report Reveals Near-Record Number of Compromises,* https://www.idtheftcenter.org/post/2022-annual-data-breach-report-reveals-near-record-number-compromises/

[26] FBI, Secret Service Warn of Targeted, Law360 (Nov.18,2019), https://www.law360.com/articles/1220974/fbisecret-service-warn-of-targeted-ransomware.

- **Update and patch your computer**. Ensure your applications and operating systems (OSs) have been updated with the latest patches. Vulnerable applications and OSs are the target of most ransomware attacks ....

- **Use caution with links and when entering website addresses.** Be careful when clicking directly on links in emails, even if the sender appears to be someone you know. Attempt to independently verify website addresses (e.g., contact your organization's helpdesk, search the internet for the sender organization's website or the topic mentioned in the email). Pay attention to the website addresses you click on, as well as those you enter yourself. Malicious website addresses often appear almost identical to legitimate sites, often using a slight variation in spelling or a different domain (e.g., .com instead of .net) ....

- **Open email attachments with caution**. Be wary of opening email attachments, even from senders you think you know, particularly when attachments are compressed files or ZIP files.

- **Keep your personal information safe.** Check a website's security to ensure the information you submit is encrypted before you provide it ....

- **Verify email senders**. If you are unsure whether or not an email is legitimate, try to verify the email's legitimacy by contacting the sender directly. Do not click on any links in the email. If possible, use a previous (legitimate) email to ensure the contact information you have for the sender is authentic before you contact them.

- **Inform yourself**. Keep yourself informed about recent cybersecurity threats and up to date on ransomware techniques. You can find information about known phishing attacks on the Anti-Phishing Working Group website. You may also want to sign up for CISA product notifications, which will alert you when a new Alert, Analysis Report, Bulletin, Current Activity, or Tip has been published.

- **Use and maintain preventative software programs**. Install antivirus software, firewalls, and email filters-and keep them updated-to reduce malicious network traffic ....[28]

132. To prevent and detect cyber-attacks or ransomware attacks Defendant could and should have implemented, as recommended by the Microsoft Threat Protection Intelligence Team, the following measures:

- **Secure internet-facing assets**

    - Apply latest security updates

[28] *See* ST 19-001:Protecting Against Ransomware (original release date Apr. 11, 2019), *available at https://readiness255.rssing.com/chan-9268821/all_p83.html*

- Use threat and vulnerability management
- Perform regular audit; remove privileged credentials;

- **Thoroughly investigate and remediate alerts**

  - Prioritize and treat commodity malware infections as potential full compromise;

- **Include IT Pros in security discussions**

  - Ensure collaboration among (security operations], [security admins], and [information technology] admins to configure servers and other endpoints securely;

- **Build credential hygiene**

  - Use [multifactor authentication] or [network level authentication] and use strong, randomized, just-in-time local admin passwords;

- **Apply principle of least-privilege**

  - Monitor for adversarial activities
  - Hunt for brute force attempts
  - Monitor for cleanup of Event Logs
  - Analyze logon events;

- **Harden infrastructure**

  - Use Windows Defender Firewall
  - Enable tamper protection
  - Enable cloud-delivered protection
  - Tum on attack surface reduction rules and [Antimalware Scan Interface] for Office [Visual Basic for Applications].[29]

Defendant Acquires, Collects, And Stores Plaintiff's the Class's PII.

133. As a condition to open an account or otherwise obtain financial services from Defendant, Plaintiffs and Class Members were required to give their sensitive and confidential PII to Defendant.

134. Defendant retains and stores this information and derives a substantial economic

[29] *Human-operated ransomware attacks: A preventable disaster,* https://www.microsoft.com/ en-us/security/blog/2020/03/05/human-operated-ransomware-attacks-a-preventable-disaster

benefit from the PII that they collect. But for the collection of Plaintiff's and Class Members' PII, Defendant would be unable to perform its services.

135. By obtaining, collecting, and storing the PII of Plaintiffs and Class Members, Defendant assumed legal and equitable duties and knew or should have known that they were responsible for protecting the PII from disclosure.

136. As a custodian of PII, Defendant knew, or should have known, the importance of safeguarding the PII entrusted to it by Plaintiffs and Class Members, and of the foreseeable consequences if its data security systems were breached, including the significant costs imposed on Plaintiffs and Class Members as a result of a breach.

Defendant Failed to Properly Protect Plaintiff's and Class Members' Private Information

137. Defendant could have prevented this Data Breach by properly securing and encrypting the systems containing the Private Information of Plaintiffs and Class Members. Alternatively, Defendant could have destroyed the data, especially for individuals with whom it had not had a relationship for a period of time.

138. Defendant's negligence in safeguarding the PII of Plaintiffs and Class Members is exacerbated by the repeated warnings and alerts directed to companies like Defendant to protect and secure sensitive data they possess.

139. Despite the prevalence of public announcements of data breach and data security compromises, Defendant failed to take appropriate steps to protect the PII of Plaintiffs and Class Members from being compromised.

140. To prevent and detect unauthorized cyber-attacks, Defendant could and should have implemented, as recommended by the United States Government, the following measures:

- Implement an awareness and training program. Because end users are targets,

employees and individuals should be aware of the threat of ransomware and how it is delivered.

- Configure firewalls to block access to known malicious IP addresses.
- Patch operating systems, software, and firmware on devices. Consider using a centralized patch management system.
- Manage the use of privileged accounts based on the principle of least privilege: no users should be assigned administrative access unless absolutely needed; and those with a need for administrator accounts should only use them when necessary.
- Configure access controls—including file, directory, and network share permissions—with least privilege in mind. If a user only needs to read specific files, the user should not have write access to those files, directories, or shares.
- Disable macro scripts from office files transmitted via email. Consider using Office Viewer software to open Microsoft Office files transmitted via email instead of full office suite applications.
- Implement Software Restriction Policies (SRP) or other controls to prevent programs from executing from common ransomware locations, such as temporary folders supporting popular Internet browsers or compression/decompression programs, including the AppData/LocalAppData folder.
- Consider disabling Remote Desktop protocol (RDP) if it is not being used.
- Use application whitelisting, which only allows systems to execute programs known and permitted by security policy.
- Execute operating system environments or specific programs in a virtualized environment.
- Categorize data based on organizational value and implement physical and logical separation of networks and data for different organizational units.[30]

Defendant Failed to Comply with FTC Guidelines

141. The Federal Trade Commission ("FTC") has promulgated numerous guides for businesses which highlight the importance of implementing reasonable data security practices.

[30] *See* How to Protect Your Networks from RANSOMWARE, at 3, *available at* https://www.fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf/view (last visited Aug. 23, 2021).

According to the FTC, the need for data security should be factored into all business decision making.

142. 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 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.[31]

143. The FTC further recommends that companies not maintain PII 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.

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

145. Defendant failed to properly implement basic data security practices, such as

[31] 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.

making a database storing Private Information available to the public without the use of a password or multifactor authentication.

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

147. Defendant were always fully aware of their obligation to protect the PII of Plaintiffs and Class Members. Defendant were also aware of the significant repercussions that would result from their failure to do so.

Defendant failed to Comply with Industry Standards

148. As shown above, experts studying cyber security routinely identify companies in the finance industry as being particularly vulnerable to cyberattacks because of the value of the PII which they collect and maintain.

149. Several best practices have been identified that at a minimum should be implemented by service providers like Defendant, including but not limited to: educating all employees; strong passwords; multi-layer security, including firewalls, anti-virus, and antimalware software; encryption, making data unreadable without a key; multi-factor authentication; backup data; and limiting which employees can access sensitive data.

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

151. The foregoing frameworks are existing and applicable industry standards in the finance industry, and Defendant failed to comply with these accepted standards, thereby opening the door to and causing the Data Breach.

As a Result of Defendant's Failure to Safeguard their Private Information, Plaintiffs and the Proposed Class now Face Significant Risk of Harm

152. Plaintiffs and Class Members have suffered injury from the access to, and misuse of, their PII that can be directly traced to Defendant.

153. The ramifications of Defendant's failure to keep Plaintiff's and the Class's PII secure are severe.

154. As a result of Defendant's failure to prevent—and to timely detect—the Data Breach, Plaintiffs and the proposed Class have suffered and will continue to suffer damages, including monetary losses, lost time, anxiety, and emotional distress. They have suffered or are at an increased risk of suffering:

a. The loss of the opportunity to control how their PII is used;

b. The diminution in value of their PII;

c. The compromise and continuing publication of their PII;

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

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

f. Delay in receipt of tax refund monies;

g. Unauthorized use of stolen PII; and

h. The continued risk to their PII, which remains in the possession of Defendant and is subject to further breaches so long as Defendant fails to undertake the appropriate measures to protect the PII in their possession.

155. One such example of criminals using PII for profit, to the detriment of Plaintiffs and the Class Members, is the development of "Fullz" packages.

156. Cyber-criminals can cross-reference two sources of PII to marry unregulated data available elsewhere to criminally stolen data with an astonishingly complete scope and degree of accuracy in order to assemble complete dossiers on individuals. These dossiers are known as "Fullz" packages.

157. The development of "Fullz" packages means that stolen PII from the Data Breach can easily be used to link and identify it to Plaintiff's and the proposed Class's phone numbers, email addresses, and other unregulated sources and identifiers. In other words, even if certain information such as emails, phone numbers, or credit card numbers may not be included in the PII stolen by the cyber-criminals in the Data Breach, criminals can easily create a Fullz package and sell it at a higher price to unscrupulous operators and criminals (such as illegal and scam telemarketers) over and over. That is exactly what is happening to Plaintiffs and members of the proposed Class, and it is reasonable for any trier of fact, including this Court or a jury, to find that Plaintiff's and other members of the proposed Class's stolen PII is being misused, and that such misuse is fairly traceable to the Data Breach.

158. 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.[32]

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

[32] Available at 2019_IC3Report.pdf (last accessed Apr. 4, 2023).

for five months.[33]

160. 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.

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

162. 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 the Class will need to be remain vigilant against unauthorized data use for years or even decades to come.

163. 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. [34] 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.

164. Defendant's failure to properly notify Plaintiffs and Class Members of the Data Breach exacerbated Plaintiff's and Class Members' injury by depriving them of the earliest ability

[33] *Id.*
[34] *See* Taking Charge, What to Do If Your Identity is Stolen, FTC, at 3 (2012), https://www.ojp.gov/ncjrs/virtual-library/abstracts/taking-charge-what-do-if-your-identity-stolen (last visited October 10, 2022).

to take appropriate measures to protect their PII and take other necessary steps to mitigate the harm caused by the Data Breach.

Plaintiff's and Class Members' Damages

165. To date, Defendant have done little to provide Plaintiffs and Class Members with relief for the damages they have suffered as a result of the Data Breach, including, but not limited to, the costs and loss of time they incurred because of the Data Breach. Defendant have only offered 12 months of inadequate credit monitoring services, despite Plaintiffs and Class Members being at risk of identity theft and fraud for the remainder of their lifetimes.

166. The 12 months of credit monitoring offered to persons whose Private Information was compromised is wholly inadequate as it fails to provide for the fact that victims of data breaches and other unauthorized disclosures commonly face multiple years of ongoing identity theft and financial fraud. What's more, Defendant place the burden squarely on Plaintiffs and Class Members by requiring them to expend time signing up for that service, as opposed to automatically enrolling all victims of this Data Breach.

167. Plaintiffs and Class Members have been damaged by the compromise of their Private Information in the Data Breach.

168. As a direct and proximate result of Defendant's conduct, Plaintiffs and Class Members have been placed at an imminent, immediate, and continuing increased risk of harm from fraud and identity theft.

169. Plaintiffs and Class Members face substantial risk of out-of-pocket fraud losses such as loans opened in their names, medical services billed in their names, tax return fraud, utility bills opened in their names, credit card fraud, and similar identity theft.

170. Plaintiffs and Class Members face substantial risk of being targeted for future

phishing, data intrusion, and other illegal schemes based on their Private Information as potential fraudsters could use that information to more effectively target such schemes to Plaintiffs and Class Members.

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

172. Defendant's delay in noticing affected persons of the theft of their Private Information prevented early mitigation efforts and compounded the harm.

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

a. Reviewing and monitoring financial and other sensitive accounts and finding fraudulent insurance claims, loans, and/or government benefits claims;

b. Purchasing credit monitoring and identity theft prevention;

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

d. Spending time on the phone with or at financial institutions and/or government agencies to dispute unauthorized and fraudulent activity in their name;

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

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

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

Information is not accessible online and that access to such data is encrypted and password protected.

175. Defendant acknowledge the harm caused to Plaintiffs and Class Members because it offers a complimentary 12-month credit monitoring program *via* Equifax.[35]

CLASS ALLEGATIONS

176. Plaintiffs bring this nationwide class action on behalf of themselves and on behalf of others similarly situated pursuant to Rule 23(b)(2), 23(b)(3), and 23(c)(4) of the Federal Rules of Civil Procedure.

177. The Nationwide Class that Plaintiffs seeks to represent is defined as follows:

> All persons whose Private Information was actually or potentially accessed or acquired by an unauthorized party as a result of the Data Breach reported by Defendant on or about May 15, 2023 (the "Nationwide Class").

178. In the alternative to the foregoing Nationwide Class, Plaintiffs seek to represent each of the following state-wide classes:

> All residents of Virginia whose Private Information was actually or potentially accessed or acquired by an unauthorized party as a result of the Data Breach reported by Defendant on or about May 15, 2023 (the "Virginia Class");
>
> All residents of North Carolina whose Private Information was actually or potentially accessed or acquired by an unauthorized party as a result of the Data Breach reported by Defendant on or about May 15, 2023 (the "North Carolina Class");
>
> All residents of Texas whose Private Information was actually or potentially accessed or acquired by an unauthorized party as a result of the Data Breach reported by Defendant on or about May 15, 2023 (the "Texas Class"); and
>
> All residents of West Virginia whose Private Information was actually or potentially accessed or acquired by an unauthorized party as a result of the Data Breach reported by Defendant on or about May 15, 2023 (the "West Virginia Class").

[35] *See* Notice Letter, *supra.*

179. Excluded from the each of the Classes are the following individuals and/or entities: Defendant and Defendant's parents, subsidiaries, affiliates, officers and directors, and any entity in which Defendant have a controlling interest; all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out; any and all federal, state or local governments, including but not limited to their departments, agencies, divisions, bureaus, boards, sections, groups, counsels and/or subdivisions; and all judges assigned to hear any aspect of this litigation, as well as their immediate family members.

180. Plaintiffs reserve the right to modify or amend the definition of the proposed classes before the Court determines whether certification is appropriate.

181. Numerosity, Fed R. Civ. P. 23(a)(1): Class Members are so numerous that joinder of all members is impracticable. According to R&B, there are hundreds of thousands of persons whose Private Information was improperly accessed in the Data Breach, and each Class is apparently identifiable within Defendant's records inasmuch as many of them have already received direct notification of the incident. R&B initially told the Maine Attorney General on May 15, 2023 that the breach impacted 286,699 people.[36] On June 6, 2023, it sent a revised notice to that same office indicating that it had impacted 231,599 people.[37]

182. Commonality, Fed. R. Civ. P. 23(a)(2) and (b)(3): Questions of law and fact common to the Classes exist and predominate over any questions affecting only individual Class Members. These include:

a. Whether and to what extent Defendant had a duty to protect the Private Information of Plaintiffs and Class Members;

b. Whether Defendant had duties not to disclose the Private Information of Plaintiffs

[36] https://apps.web.maine.gov/online/aeviewer/ME/40/6a11760a-5f54-4fa7-b222-f74eed5cf516.shtml (last visited Aug. 18, 2023).
[37] https://apps.web.maine.gov/online/aeviewer/ME/40/a5270b26-3247-48fd-ab4a-f68eb29248df.shtml (last visited Aug. 18, 2023).

and Class Members to unauthorized third parties;

c. Whether Defendant failed to adequately safeguard the Private Information of Plaintiffs and Class Members;

d. Whether and when Defendant actually learned of the Data Breach;

e. Whether Defendant adequately, promptly, and accurately informed Plaintiffs and Class Members that their PII had been compromised;

f. Whether Defendant violated the law by failing to promptly notify Plaintiffs and Class Members that their PII had been compromised;

g. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

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

i. Whether Plaintiffs and Class Members are entitled to actual, consequential, and/or nominal damages as a result of Defendant's wrongful conduct;

j. Whether Plaintiffs and Class Members are entitled to restitution as a result of Defendant's wrongful conduct; and

k. Whether Plaintiffs and Class Members are entitled to injunctive relief to redress the imminent and currently ongoing harm faced as a result of the Data Breach.

183. Typicality, Fed. R. Civ. P. 23(a)(3): Plaintiff's claims are typical of those of other Class Members because all had their PII compromised as a result of the Data Breach, due to Defendant's misfeasance.

184. Policies Generally Applicable to the Class: This class action is also appropriate for certification because Defendant have acted or refused to act on grounds generally applicable to the Class, thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward the Class Members and making final injunctive relief appropriate with respect to the Class as a whole. Defendant's policies challenged herein apply to and affect Class Members uniformly and Plaintiff's challenge of these policies hinges on Defendant's conduct with respect

to the Class as a whole, not on facts or law applicable only to Plaintiff.

185. Adequacy, Fed. R. Civ. P. 23(a)(4): Plaintiffs will fairly and adequately represent and protect the interests of the Class Members in that Plaintiffs have no disabling conflicts of interest that would be antagonistic to those of the other Members of the Class. Plaintiffs seek no relief that is antagonistic or adverse to the Members of the Class and the infringement of the rights and the damages Plaintiffs have suffered are typical of other Class Members. Plaintiffs have also retained counsel experienced in complex class action litigation, and Plaintiffs intend to prosecute this action vigorously.

186. Superiority and Manageability, Fed. R. Civ. P. 23(b)(3): Class litigation is an appropriate method for fair and efficient adjudication of the claims involved. Class action treatment is superior to all other available methods for the fair and efficient adjudication of the controversy alleged herein; it will permit a large number of Class Members to prosecute their common claims in a single forum simultaneously, efficiently, and without the unnecessary duplication of evidence, effort, and expense that hundreds of individual actions would require. Class action treatment will permit the adjudication of relatively modest claims by certain Class Members, who could not individually afford to litigate a complex claim against large corporations, like Defendant. Further, even for those Class Members who could afford to litigate such a claim, it would still be economically impractical and impose a burden on the courts.

187. The nature of this action and the nature of laws available to Plaintiffs and Class Members make the use of the class action device a particularly efficient and appropriate procedure to afford relief to Plaintiffs and Class Members for the wrongs alleged because Defendant would necessarily gain an unconscionable advantage since they would be able to exploit and overwhelm the limited resources of each individual Class Member with superior financial and legal resources;

the costs of individual suits could unreasonably consume the amounts that would be recovered; proof of a common course of conduct to which Plaintiffs were exposed is representative of that experienced by the Class and will establish the right of each Class Member to recover on the cause of action alleged; and individual actions would create a risk of inconsistent results and would be unnecessary and duplicative of this litigation.

188. The litigation of the claims brought herein is manageable. Defendant's uniform conduct, the consistent provisions of the relevant laws, and the ascertainable identities of Class Members demonstrates that there would be no significant manageability problems with prosecuting this lawsuit as a class action.

189. Adequate notice can be given to Class Members directly using information maintained in Defendant's records.

190. Unless a Class-wide injunction is issued, Defendant may continue in their failure to properly secure the Private Information of Class Members, Defendant may continue to refuse to provide proper notification to Class Members regarding the Data Breach, and Defendant may continue to act unlawfully as set forth in this Complaint.

191. Further, Defendant have acted or refused to act on grounds generally applicable to the Classes and, accordingly, final injunctive or corresponding declaratory relief with regard to the Class Members as a whole is appropriate under Rule 23(b)(2) of the Federal Rules of Civil Procedure.

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

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

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

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

d. Whether an implied contract existed between Defendant on the one hand, and Plaintiffs and Class Members on the other, and the terms of that implied contract;

e. Whether Defendant breached the implied contract;

f. Whether Plaintiffs and Class members were third party beneficiaries of contracts that were breached.

g. Whether Defendant violated the Virginia Consumer Protection Act.

h. Whether Defendant violated the Virginia Personal Information Breach Notification Act.

i. Whether Defendant adequately and accurately informed Plaintiffs and Class Members that their Private Information had been compromised;

j. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

k. Whether Class Members are entitled to actual, consequential, and/or nominal damages, and/or injunctive relief as a result of Defendant's wrongful conduct.

CAUSES OF ACTION

COUNT I
NEGLIGENCE
(On Behalf of Plaintiffs and the Nationwide Class or, Alternatively, the Virginia, North Carolina, Texas and West Virginia Classes)

193. Plaintiffs and the Class repeat and re-allege each allegation as if fully set forth herein.

194. Plaintiffs and the Class entrusted Defendant with their Private Information.

195. Plaintiffs and the Class entrusted their Private Information to Defendant on the premise and with the understanding that Defendant would safeguard their information, use their information for business purposes only, and/or not disclose their Private Information to unauthorized third parties.

196. Defendant had full knowledge of the sensitivity of the Private Information and the types of harm that Plaintiffs and the Class could and would suffer if the Private Information were wrongfully disclosed.

197. Defendant knew or reasonably should have known that the failure to exercise due care in the collecting, storing, and using of the Private Information of Plaintiffs and the Class involved an unreasonable risk of harm to Plaintiffs and the Class, even if the harm occurred through the criminal acts of a third party.

198. By accepting, storing, and maintaining Plaintiff's and Class Members' Private Information, Defendant undertook a duty to exercise reasonable care in safeguarding, securing, and protecting such information from being compromised, lost, stolen, misused, and/or disclosed to unauthorized parties. This duty includes, among other things, designing, maintaining, and testing Defendant's security protocols to ensure that the Private Information of Plaintiffs and the Class Members in Defendant's possession was adequately secured and protected.

199. By accepting, storing, and maintaining Plaintiff's and Class Members' Private Information, Defendant also had a duty to exercise appropriate clearinghouse practices to remove Private Information they were no longer required to retain pursuant to regulations.

200. By accepting, storing, and maintaining Plaintiff's and Class Members' Private Information, Defendant also had a duty to have procedures in place to detect and prevent the improper access and misuse of the Private Information of Plaintiffs and the Class.

201. Defendant's duty to use reasonable security measures arose as a result of the special relationship that existed between Defendant and Plaintiffs and the Class. That special relationship arose because Plaintiffs and the Class entrusted Defendant with their confidential Private Information, a necessary part of obtaining services from Defendant.

202. Defendant were subject to an "independent duty," untethered to any contract between Defendant and Plaintiffs or the Class.

203. A breach of security, unauthorized access, and resulting injury to Plaintiffs and the Class was reasonably foreseeable, due to the nature of Defendant's industry, and particularly in light of Defendant's inadequate security practices.

204. Plaintiffs and the Class were the foreseeable and probable victims of any inadequate security practices and procedures. Defendant knew or should have known of the inherent risks in collecting and storing the Private Information of Plaintiffs and the Class, the critical importance of providing adequate security of that Private Information, and the necessity for encrypting Private Information stored on Defendant's systems.

205. Defendant's own conduct created a foreseeable risk of harm to Plaintiffs and the Class. Defendant's misconduct included, but was not limited to, their failure to take the steps and opportunities to prevent the Data Breach as set forth herein. Defendant's misconduct also included their decisions not to comply with industry standards for the safekeeping of the Private Information of Plaintiffs and the Class, including basic encryption techniques freely available to Defendant.

206. Defendant knew or should have known that Plaintiff's and Class Members' Private Information was stored on their database and were or should have been aware of the extreme risks associated with failing to properly safeguard Plaintiff's and Class Members' Private Information.

207. Despite being aware of the likelihood that Defendant's databases were vulnerable,

not secure, and likely to be attacked by cybercriminals, Defendant failed to correct, update, or upgrade their security protections, thus causing the Data Breach.

208. Plaintiffs and the Class had no ability to protect their Private Information that was in, and possibly remains in, Defendant's possession.

209. Defendant were in the best position to protect against the harm suffered by Plaintiffs and the Class as a result of the Data Breach.

210. Defendant had and continues to have a duty to adequately disclose that the Private Information of Plaintiffs and the Class within Defendant's possession might have been compromised, how it was compromised, and precisely the types of data that were compromised and when. Such notice was necessary to allow Plaintiffs and the Class to take steps to prevent, mitigate, and repair any identity theft and the fraudulent use of their Private Info by third parties.

211. Defendant had a duty to employ proper procedures to prevent the unauthorized dissemination of the Private Information of Plaintiffs and the Class.

212. Defendant improperly and inadequately safeguarded the Private Information of Plaintiffs and the Class in deviation of standard industry rules, regulations, and practices at the time of the Data Breach.

213. Defendant, through their actions and/or omissions, unlawfully breached their duties to Plaintiffs and the Class by failing to implement industry protocols and exercise reasonable care in protecting and safeguarding the Private Information of Plaintiffs and the Class during the time the Private Information was within Defendant's possession or control.

214. Defendant failed to heed industry warnings and alerts to provide adequate safeguards to protect the Private Information of Plaintiffs and the Class in the face of increased risk of theft.

215. Defendant, through their actions and/or omissions, unlawfully breached their duty to Plaintiffs and the Class by failing to have appropriate procedures in place to detect and prevent dissemination of Private Information.

216. Defendant breached their duty to exercise appropriate clearinghouse practices by failing to remove Private Information they were no longer required to retain pursuant to regulations.

217. Defendant, through their actions and/or omissions, unlawfully breached their duty to adequately and timely disclose to Plaintiffs and the Class the existence and scope of the Data Breach.

218. But for Defendant's wrongful and negligent breach of duties owed to Plaintiffs and the Nationwide Class, the Private Information of Plaintiffs and the Class would not have been compromised.

219. Plaintiffs and Class Members suffered an injury when their Private Information was accessed by unknown third parties.

220. There is a close causal connection between Defendant's failure to implement security measures to protect the Private Information of Plaintiffs and the Class and the harm, and increased risk of imminent harm, suffered by Plaintiffs and the Nationwide Class.

221. The Private Information of Plaintiffs and Class Members was lost and accessed as the proximate result of Defendant's failure to exercise reasonable care in safeguarding such Private Information by adopting, implementing, and maintaining appropriate security measures.

222. As a direct and proximate result of Defendant's negligence, Plaintiffs and the Class have suffered and will suffer injury, including but not limited to, the following: (i) actual identity theft; (ii) the loss of the opportunity of how their Private Information is used; (iii) the compromise,

publication, and/or theft of their Private Information; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their Private Information; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the present and continuing consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from tax fraud and identity theft; (vi) costs associated with placing freezes on credit reports; (vii) the continued risk to their Private Information, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fail to undertake appropriate and adequate measures to protect the Private Information of Plaintiffs and the Class; and (viii) present and continuing costs in terms of time, effort, and money that has been and will be expended to prevent, detect, contest, and repair the impact of the Private Information compromised as a result of the Data Breach for the remainder of the lives of Plaintiffs and the Class.

223. As a direct and proximate result of Defendant's negligence, Plaintiffs and the Class have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

224. Additionally, as a direct and proximate result of Defendant's negligence Plaintiffs and the Class have suffered and will suffer the continued risks of exposure of their Private Information, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fail to undertake appropriate and adequate measures to protect the Private Information in their continued possession.

225. As a direct and proximate result of Defendant's negligence, Plaintiffs and the Class

are entitled to recover actual, consequential, and nominal damages.

COUNT II
NEGLIGENCE PER SE – Based on Section 5 of the FTC Act
(On Behalf of Plaintiffs and the Nationwide Class or, Alternatively, the Virginia, North Carolina, Texas and West Virginia Classes)

226. Plaintiffs and the Class repeat and re-allege each allegation in the Complaint as if fully set forth herein.

227. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendant, of failing to use reasonable measures to protect PII. The FTC publications and orders described above also form part of the basis of Defendant's duty in this regard.

228. Defendant violated Section 5 of the FTC Act by failing to use reasonable measures to protect PII and not complying with applicable industry standards, as described in detail herein. Defendant's conduct was particularly unreasonable given the nature and amount of PII it obtained and stored and the foreseeable consequences of the immense damages that would result to Plaintiffs and the Class.

229. Defendant's violation of Section 5 of the FTC Act constitutes negligence *per se*.

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

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

232. As a direct and proximate result of Defendant's negligence *per se*, Plaintiffs and the Class have suffered and will suffer injury, including but not limited to: (i) actual identity theft;

(ii) the loss of the opportunity of how their PII is used; (iii) the compromise, publication, and/or theft of their PII; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the present and continuing consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from tax fraud and identity theft; (vi) costs associated with placing freezes on credit reports; (vii) the continued risk to their PII, which remains in Defendants' possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII of Plaintiffs and the Class; and (viii) present and continuing costs in terms of time, effort, and money that has been and will be expended to prevent, detect, contest, and repair the impact of the PII compromised as a result of the Data Breach for the remainder of the lives of Plaintiffs and the Class.

233. As a direct and proximate result of Defendant's negligence *per se*, Plaintiffs and the Class have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

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

235. As a direct and proximate result of Defendant's negligence *per se*, Plaintiffs and

the Class are entitled to recover actual, consequential, and nominal damages.

COUNT III
NEGLIGENCE PER SE – Based on the Virginia Personal Information Breach Notification Act
(On Behalf of Plaintiffs and the Virginia Class)

236. Plaintiffs and the Class repeat and re-allege each allegation in the Complaint as if fully set forth herein.

237. Defendant is required to accurately notify Plaintiffs and Class Members following discovery or notification of a breach of its data security system if unencrypted or unredacted PII was or is reasonably believed to have been accessed and acquired by an unauthorized person who will, or it is reasonably believed who will, engage in identity theft or another fraud, without unreasonable delay under Va. Code Ann. § 18.2-186.6(B).

238. Defendant is an entity that owns or licenses computerized data that includes PII as defined by Va. Code Ann. § 18.2-186.6(B).

239. Plaintiffs' and Class Members' PII includes PII as covered under Va. Code Ann. § 18.2-186.6(A).

240. Because Defendant discovered a breach of its security system in which unencrypted or unredacted PII was or is reasonably believed to have been accessed and acquired by an unauthorized person, who will, or it is reasonably believed who will, engage in identity theft or another fraud, Defendant had an obligation to disclose the data breach in a timely and accurate fashion as mandated by Va. Code Ann. § 18.2-186.6(B).

241. By failing to disclose the Defendant data breach in a timely and accurate manner, Defendant violated Va. Code Ann. § 18.2-186.6(B).

242. As a direct and proximate result of Defendant's violations of Va. Code Ann. § 18.2-186.6(B), Plaintiffs and Class Members suffered damages, as described above.

243. The harm that occurred as a result of the Data Breach is the type of harm the Virginia Personal Information Breach Notification Act was intended to guard against.

COUNT IV
BREACH OF IMPLIED CONTRACT
(On Behalf of Plaintiffs and the Nationwide Class or, Alternatively, the Virginia, North Carolina, Texas and West Virginia Classes)

244. Plaintiffs and the Class repeat and re-allege each allegation in the Complaint as if fully set forth herein.

245. Plaintiffs and Class Members were required to provide Defendant with their Private Information.

246. By Plaintiffs and Class Members providing their Private Information, and by Defendant accepting this Private Information, the parties mutually assented to implied contracts. These implied contracts included an implicit agreement and understanding that (1) Defendant would adequately safeguard Plaintiff's and Class Members' Private Information from foreseeable threats, (2) that Defendant would delete the information of Plaintiffs and Class Members once it no longer had a legitimate need; and (3) that Defendant would provide Plaintiffs and Class Members with notice within a reasonable amount of time after suffering a data breach.

247. On information and belief, at all relevant times Defendant promulgated, adopted, and implemented written privacy policies whereby it expressly promised Plaintiffs and Class Members that it would only disclose PII under certain circumstances, none of which relate to the Data Breach.

248. On information and belief, Defendant further promised to comply with industry standards and to make sure that Plaintiff's and Class Members' PII would remain protected.

249. Defendant provided consideration by providing services, while Plaintiffs and Class

Members provided consideration by providing valuable property—i.e., their Private Information. Defendant benefitted from the receipt of this Private Information by increasing profit from additional business.

250. Plaintiffs and the Class fully performed their obligations under the implied contracts with Defendant.

251. Defendant materially breached their implied contracts with Plaintiffs and Class Members when it (1) placed their Private Information on an unsecured computer system that could (and later was) accessed by unauthorized and (2) waited an unreasonably long time to notify them of the Data Breach. It is common sense that Plaintiffs and Class Members would not have provided Defendant with their Private Information had they known that Defendant would not implement basic data security measures or that it would wait several months to notify them of a data breach involving their Private Information.

252. Defendant's breaches of contract have caused Plaintiffs and Class Members to suffer damages from the lost benefit of their bargain, out of pocket monetary losses and expenses, loss of time, and diminution of the value of their Private Information.

253. As a direct and proximate result of Defendant's above-described breach of implied contract, Plaintiffs 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; time spent scrutinizing bank statements, credit card statements, and credit reports; expenses and/or time spent initiating fraud alerts, decreased credit scores and ratings; lost work

time; and other economic and non-economic harm.

COUNT V
BREACH OF CONTRACTS TO WHICH PLAINTIFFS AND CLASS MEMBERS WERE INTENDED THIRD PARTY BENEFICIARIES
(On Behalf of Plaintiffs and the Nationwide Class or, Alternatively, the Virginia, North Carolina, Texas and West Virginia Classes)

254. Plaintiffs and the Class repeat and re-allege each allegation as if fully set forth herein.

255. Defendant had valid contracts to provide debt collection services to various clients, and a principal purpose of those contracts was to securely store, transmit and safeguard the private information of Plaintiffs and Class Members.

256. R&B's website assures these customers that it has reasonable data security measures in place, stating "your information is secure" with it.[38]

257. Plaintiffs and Class Members are intended third party beneficiaries of these agreements because recognizing them as such is appropriate to effectuate the intentions of the parties, and the circumstances indicate that Defendant intended to give the beneficiaries the benefit of the promised performance.

258. Defendant knew that if it were to breach these contracts with its clients, the clients' customers—Plaintiffs and Class Members—would be harmed.

259. It was intended by Defendant and its clients at the time the contracts were made that Defendant would assume a direct obligation to protect Plaintiff's and the Class's Private Information.

260. Defendant breached these contractual obligations by allowing the data breach to occur, and failing to use reasonable data security measures or implement adequate protocols and

[38] https://creditcontrol.net/services/ (last visited Aug. 17, 2023).

employee training sufficient to protect Plaintiff's Private Information from unauthorized disclosure to third parties, as otherwise set forth herein.

261. Defendant's breach caused foreseeable and material damages to Plaintiffs and Class Members.

COUNT VI
UNJUST ENRICHMENT
(On Behalf of Plaintiffs and the Nationwide Class or, Alternatively, the Virginia, North Carolina, Texas and West Virginia Classes)

262. Plaintiffs and the Class repeat and re-allege each allegation as if fully set forth herein. This claim is pled in the alternative to the contract based counts.

263. Plaintiffs and Class Members conferred a monetary benefit on Defendant, by providing Defendant with their valuable Private Information.

264. Defendant enriched itself by saving the costs they reasonably should have expended on data security measures to secure Plaintiff's and Class Members' Private Information.

265. Instead of providing a reasonable level of security that would have prevented the Data Breach, Defendant instead calculated to avoid their data security obligations at the expense of Plaintiffs and Class Members by utilizing cheaper, ineffective security measures. Plaintiffs and Class Members, on the other hand, suffered as a direct and proximate result of Defendant's failure to provide the requisite security.

266. Under the principles of equity and good conscience, Defendant should not be permitted to retain the monetary value of the benefit belonging to Plaintiffs and Class Members, because Defendant failed to implement appropriate data management and security measures that are mandated by industry standards.

267. Defendant acquired the monetary benefit and PII through inequitable means in that they failed to disclose the inadequate security practices previously alleged.

268. If Plaintiffs and Class Members knew that Defendant had not secured their PII, they would not have agreed to provide their PII to Defendant (or to the merchants that subsequently provided it to R&B).

269. Plaintiffs and Class Members have no adequate remedy at law.

270. As a direct and proximate result of Defendant's conduct, Plaintiffs and Class Members have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity how their Private Information is used; (iii) the compromise, publication, and/or theft of their PII; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, and/or unauthorized use of their Private Information; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (vi) the continued risk to their Private Information, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fail to undertake appropriate and adequate measures to protect Private Information in their continued possession and (vii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the Private Information compromised as a result of the Data Breach for the remainder of the lives of Plaintiffs and Class Members.

271. As a direct and proximate result of Defendant's conduct, Plaintiffs and Class Members have suffered and will continue to suffer other forms of injury and/or harm. Defendant should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiffs and Class Members, proceeds that they unjustly received from them.

COUNT VII
VIRGINIA CONSUMER PROTECTION ACT,
VA. CODE ANN. §§ 59.1-196, ET SEQ.
(On Behalf of the Virginia Class)

272. Plaintiffs and the Class repeat and re-allege each allegation as if fully set forth herein.

273. The Virginia Consumer Protection Act prohibits "[u]sing any . . . deception, fraud, false pretense, false promise, or misrepresentation in connection with a consumer transaction." Va. Code Ann. § 59.1-200(14).

274. Defendant is a "person" as defined by Va. Code Ann. § 59.1-198.

275. Defendant is a "supplier," as defined by Va. Code Ann. § 59.1-198.

276. Defendant engaged in the complained-of conduct in connection with "consumer transactions" with regard to "goods" and "services," as defined by Va. Code Ann. § 59.1-198. Defendant advertised, offered, or sold goods or services used primarily for personal, family or household purposes; or relating to an individual's finding or obtaining employment (such as furnishing credit reports to prospective employers).

277. Defendant engaged in deceptive acts and practices by using deception, fraud, false pretense, false promise, and misrepresentation in connection with consumer transactions, including:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiffs' and Class Members' PII, which was a direct and proximate cause of the Data Breach;

b. Failing to identify and remediate foreseeable security and privacy risks and adequately improve security and privacy measures despite knowing the risk of

cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Class Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, which was a direct and proximate cause of the Data Breach;

d. Misrepresenting that they would protect the privacy and confidentiality of Plaintiffs' and Class Members' PII, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that they would comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Class Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45;

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

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

278. Defendant intended to mislead Plaintiffs and Class Members and induce them to rely on its misrepresentations and omissions.

279. Defendant's representations and omissions were material because they were likely to deceive reasonable consumers, including Plaintiffs and Class Members, about the adequacy of Defendant's computer and data security and the quality of the Defendant brand.

280. Had Defendant disclosed to Plaintiffs and Class Members that its data systems were not secure and, thus, vulnerable to attack, Defendant would have been unable to continue in business and it would have been forced to adopt reasonable data security measures and comply with the law. Defendant was trusted with sensitive and valuable PII regarding millions of consumers, including Plaintiffs and the Class. Defendant accepted the responsibility of protecting the data while keeping the inadequate state of its security controls secret from the public. Accordingly, Plaintiffs and the Class Members acted reasonably in relying on Defendant's misrepresentations and omissions, the truth of which they could not have discovered.

281. In Defendant had a duty to disclose these facts due to the circumstances of this case, the sensitivity and extensivity of the PII in its possession, and the generally accepted professional standards. Such a duty is implied by law due to the nature of the relationship between consumers including Plaintiffs and the Class – and Defendant, because consumers are unable to fully protect their interests with regard to their data, and placed trust and confidence in Defendant. Defendant's duty to disclose also arose from its:

a. Possession of exclusive knowledge regarding the security of the data in its systems;

b. Active concealment of the state of its security; and/or

c. Incomplete representations about the security and integrity of its computer and data systems, and its prior data breaches, while purposefully withholding material facts from Plaintiffs and the Class that contradicted these representations.

282. The above-described deceptive acts and practices also violated the following provisions of VA Code § 59.1-200(A):

a. Misrepresenting that goods or services have certain characteristics, uses, or

benefits;

b. Misrepresenting that goods or services are of a particular standard, quality, grade, style, or model; and

c. Advertising goods or services with intent not to sell them as advertised, or with intent not to sell them upon the terms advertised;

d. Using any other deception, fraud, false pretense, false promise, or misrepresentation in connection with a consumer transaction.

283. Defendant acted intentionally, knowingly, and maliciously to violate Virginia's Consumer Protection Act, and recklessly disregarded Plaintiffs and Class Members' rights. Defendant's numerous past data breaches put it on notice that its security and privacy protections were inadequate. An award of punitive damages would serve to punish Defendant for its wrongdoing, and warn or deter others from engaging in similar conduct.

284. As a direct and proximate result of Defendant's deceptive acts or practices, Plaintiffs and Class Members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, as described herein, including but not limited to fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; loss of value of their PII; overpayment for Defendant's services; loss of the value of access to their PII; and the value of identity protection services made necessary by the Breach.

285. Defendant's violations present a continuing risk to Plaintiffs and Class Members as well as to the general public.

286. Plaintiffs and Class Members seek all monetary and non-monetary relief allowed by law, including actual damages; statutory damages in the amount of $1,000 per violation if the

conduct is found to be willful or, in the alternative, $500 per violation; restitution, injunctive relief; punitive damages; and attorneys' fees and costs.

COUNT VIII
VIOLATIONS OF THE NORTH CAROLINA UNFAIR AND DECEPTIVE TRADE PRACTICES ACT ("UDTPA")
N.C. Gen. Stat. §§75-1, *et seq*.
(On Behalf of the North Carolina Class)

287. Plaintiffs and the Class repeat and re-allege each allegation as if fully set forth herein.

288. Plaintiff Powers brings this action individually and on behalf of the members of the North Carolina Subclass.

289. The North Carolina Unfair and Deceptive Trade Practices Act ("UDTPA") was created to protect North Carolina consumers from unfair or deceptive business practices.

290. R&B has engaged in immoral, unethical, oppressive, unscrupulous, substantially injurious and misleading commercial practices, with the intent to deceive consumers.

291. Plaintiffs and North Carolina Subclass members reasonably relied on R&B to reasonably safeguard their sensitive PII. As discussed above, R&B failed to do so.

292. Accordingly, pursuant to the aforementioned statutes, Plaintiff Powers and North Carolina Subclass members are entitled to recover their actual damages, which can be calculated with a reasonable degree of certainty using sufficiently definitive and objective evidence. In addition, given the nature of R&B's conduct in the face of several other breaches, Plaintiffs and North Carolina Subclass members are entitled to recover statutory, exemplary, treble, and/or punitive damages, together with interest, cost of suit, and attorneys' fees based on the amount of time reasonable expended and equitable relief necessary, and all such other relief as the Court deems proper.

COUNT IX
WEST VIRGINIA CONSUMER CREDIT PROTECTION ACT
W. Va. Code Ann. § 46A-6-101, *et seq.*
(On Behalf of the West Virginia Class)

293. Plaintiffs and the Class repeat and re-allege each allegation as if fully set forth herein.

294. The West Virginia Consumer Credit Protection Act ("WVCCPA") was created to protect West Virginia consumers from deceptive and unfair business practices.

295. R&B's conduct described herein constitutes unfair methods of competition and unfair or deceptive acts or practices in the conduct of any trade or commerce in West Virginia, making it unlawful under W. Va. Code Ann. §§ 46A-6-104.

296. Plaintiffs and West Virginia Subclass members suffered ascertainable losses of money or property as the result of the use or employment of a method, act or practice declared unlawful by W. Va. Code Ann. § 46A-6-102(7). Plaintiffs and West Virginia Subclass members acted as reasonable consumers would have acted under the circumstances.

297. Accordingly, pursuant to W. Va. Code § 46A-6-106(a), Plaintiffs and West Virginia Subclass members are entitled to recover their actual damages in the amount to be determined at trial. In addition, given the nature of R&B's conduct, Plaintiffs and West Virginia Subclass Members are entitled to recover statutory damages of $1,000 per violation for the knowing and willful violation of the WVCCPA and attorneys' fees based on the amount of time reasonably expended and equitable relief necessary or proper to protect them from R&B's unlawful conduct.

COUNT X
DECLARATORY AND INJUNCTIVE RELIEF
(On Behalf of Plaintiffs and the Nationwide Class or, Alternatively, the Virginia, North Carolina, Texas and West Virginia Classes)

298. Plaintiffs and the Class repeat and re-allege each allegation as if fully set forth herein.

299. Plaintiffs pursues this claim under the Federal Declaratory Judgment Act, 28 U.S.C. § 2201.

300. Defendant owes a duty of care to Plaintiffs and Class Members that require it to adequately secure Plaintiff's and Class Members' Private Information.

301. Defendant failed to fulfill their duty of care to safeguard Plaintiff's and Class Members' Private Information.

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

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

304. Plaintiff, therefore, seeks a declaration (1) that Defendant's existing data security measures do not comply with their contractual obligations and duties of care to provide adequate data security, and (2) that to comply with their contractual obligations and duties of care, Defendant must implement and maintain reasonable security measures, including, but not limited to, the following:

a. Ordering that Defendant engage internal security personnel to conduct testing, including audits on Defendant's systems, on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors;

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

c. Ordering that Defendant audit, test, and train their security personnel and employees regarding any new or modified data security policies and procedures;

d. Ordering that Defendant purge, delete, and destroy, in a reasonably secure manner, any Private Information not necessary for their provision of services;

e. Ordering that Defendant conduct regular database scanning and security checks; and

f. Ordering that Defendant routinely and continually conduct internal training and education to inform internal security personnel and employees how to safely share and maintain highly sensitive personal information, including but not limited to, Plaintiffs and Class Members' Personally Identifiable Information.

PRAYER FOR RELIEF

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

A. For an Order certifying the Class, and appointing Plaintiffs and Counsel to represent the Class;

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

Plaintiffs and Class Members, and from refusing to issue prompt, complete, any accurate disclosures to Plaintiffs and Class Members;

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

i. prohibiting Defendant from engaging in the wrongful and unlawful acts described herein;

ii. requiring Defendant to protect, including through encryption, all data collected through the course of their business in accordance with all applicable regulations, industry standards, and federal, state or local laws;

iii. requiring Defendant to delete, destroy, and purge the personally identifying information of Plaintiffs and Class Members unless Defendant can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiffs and Class Members;

iv. requiring Defendant to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of the PII of Plaintiffs and Class Members;

v. requiring Defendant to engage independent third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third-party

security auditors;

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

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

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

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

x. requiring Defendant to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon the employees' respective responsibilities with handling personally identifiable information, as well as protecting the personally identifiable information of Plaintiffs and Class Members;

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

xii. requiring Defendant to implement a system of tests to assess their respective employees' knowledge of the education programs discussed in the

preceding subparagraphs, as well as randomly and periodically testing employees compliance with Defendant's policies, programs, and systems for protecting personally identifying information;

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

xiv. requiring Defendant to meaningfully educate all Class Members about the threats that they face as a result of the loss of their confidential personally identifiable information to third parties, as well as the steps affected individuals must take to protect themselves;

xv. requiring Defendant to implement logging and monitoring programs sufficient to track traffic to and from Defendant's servers; and for a period of 10 years, appointing a qualified and independent third party assessor to conduct a SOC 2 Type 2 attestation on an annual basis to evaluate Defendant's compliance with the terms of the Court's final judgment, to provide such report to the Court and to counsel for the class, and to report any deficiencies with compliance of the Court's final judgment;

D. For an award of damages, including, but not limited to, actual, consequential, and nominal damages, as allowed by law in an amount to be determined;

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

F. For prejudgment interest on all amounts awarded; and

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

DEMAND FOR JURY TRIAL

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

Date: August 18, 2023

Respectfully submitted,

/s/ David Hilton Wise
David Hilton Wise (VA Bar No. 30828)
Joseph M. Langone (VA Bar No. 43543)
WISE LAW FIRM PLC
10640 Page Avenue, Suite 320
Fairfax, Virginia 22030
Phone: 703-934-6377
dwise@wiselaw.pro
jlangone@wiselaw.pro

Liaison Counsel

Bryan L. Bleichner*
Philip J. Krzeski*
CHESTNUT CAMBRONNE PA
100 Washington Avenue South, Suite 1700
Minneapolis, MN 55401
Phone: (612) 339-7300
Fax: (612) 336-2940
bbliechner@chestnutcambronne.com
pkrzeski@chestnutcambronne.com

Jonathan Shub*
Benjamin F. Johns*
Samantha Holbrook*
SHUB & JOHNS LLC
Four Tower Bridge 200 Barr Harbor Drive, Suite 400 Conshohocken, PA 19428
Telephone: (610) 477-8380
Fax: (856) 210-9088
bjohns@shublawyers.com
jshub@shublawyers.com
sholbrook@shublawyers.com

Gary M. Klinger*
David K. Lietz*
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN, PLLC
227 W. Monroe Street, Suite 2100
Chicago, IL 60606
Telephone: (866) 252-0878
gklinger@milberg.com
dlietz@milberg.com

Interim Co-Lead Class Counsel

Josh Sanford*
SANFORD LAW FIRM, PLLC
10800 Financial Centre, Pkwy., Ste. 510
Little Rock, Arkansas 72211
Phone: (501) 787-2040
josh@sanfordlaw.com

Joseph M. Lyon*
THE LYON LAW FIRM
2754 Erie Ave.
Cincinnati, Ohio 45208
Phone: (513) 381-2333
Fax: (513) 766-9011
jlyon@thelyonfirm.com

Joshua Lee Jewett (VSB No. 76684)
PIERCE MCCOY, PLLC
101 W. Main St., Ste. 101
Norfolk, VA 23510
Tel: (757) 286-2903
Fax: (757) 257-0387
jjewett@piercemccoy.com

Lee A. Floyd, VSB #88459
Justin M. Sheldon, VSB #82632
BREIT BINIAZAN, PC
2100 East Cary Street, Suite 310
Richmond, Virginia 23223
Telephone: (804) 351-9040
Facsimile: (757) 670-3939
Lee@bbtrial.com
Justin@bbtrial.com

David K. Lietz*
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN, PLLC
5101 Wisconsin Ave. NW, Suite 305
Washington, D.C. 20016
Telephone: (202) 429-2290
dlietz@milberg.com

Lee A. Floyd, VSB #88459
Justin M. Sheldon, VSB #82632
BREIT BINIAZAN, PC
2100 East Cary Street, Suite 310
Richmond, Virginia 23223
Telephone: (804) 351-9040
Facsimile: (757) 670-3939
Lee@bbtrial.com
Justin@bbtrial.com

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

Michael R. Hirsh, VSB #36569
HIRSH LAW OFFICE, LLC
2295 Towne Lake Pkwy.
Suite 116-181
Woodstock, GA 30189
678-623-9907
Micahel@Hirsh.law

Mason A. Barney*
Tyler J. Bean*
SIRI & GLIMSTAD LLP
745 Fifth Avenue, Suite 500
New York, New York 10151
Tel: (212) 532-1091
mbarney@sirillp.com
tbean@sirillp.com

Gary E. Mason*
Danielle L. Perry*
Lisa A. White*
MASON LLP
5335 Wisconsin Avenue, NW, Suite 640
Washington, DC 20015
Tel: (202) 429-2290
gmason@masonllp.com
dperry@masonllp.com
lwhite@masonllp.com

Steven T. Webster (VA Bar No. 31975)
300 N. Washington St., Suite 404
Alexandria, Virginia 22314
(888) 987-9991
swebster@websterbook.com

John A. Yanchunis
Marcio W. Valladares
Ra O. Amen
MORGAN & MORGAN
COMPLEX LITIGATION GROUP
201 North Franklin Street 7th Floor
Tampa, Florida 33602
T: (813) 223-5505
F: (813) 223-5402
JYanchunis@forthepeople.com
MValladares@forthe people.com
Ramen@forthepeople.com

Additional Counsel for Plaintiffs

**admitted pro hac vice*

CERTIFICATE OF SERVICE

The undersigned hereby certifies that on this 18th day of August 2023, a true and correct copy of the foregoing was served electronically through CM/ECF to all counsel of record and by email to Defendant's counsel of record:

Jill H. Fertel, Esq.
Ernest F. Koschineg, Esq.
Antima G. Chackraborty, Esq.
CIPRIANI & WERNER P.C.
450 Sentry Parkway, Suite 200
Blue Bell, PA 19422
P: 610-567-0715
JFertel@c-wlaw.com
AChakraborty@c-wlaw.com

Counsel for Defendant R&B Corporation of Virginia d/b/a Credit Control Corporation

/s/ David Hilton Wise
David Hilton Wise (VA Bar No. 30828)