UNTIED STATES DISTRICT COURT
FOR THE DISTRICT OF SOUTH CAROLINA
COLUMBIA DIVISION

DODIE WADEN, individually and on behalf of all others similarly situated, Plaintiff, v. PROGRESSIVE CASUALTY INSURANCE COMPANY, Defendant.	**CLASS ACTION COMPLAINT** **Case No.** 3:24-cv-00260-CMC **DEMAND FOR JURY TRIAL**

CLASS ACTION COMPLAINT

Plaintiff Dodie Waden ("Plaintiff"), individually and on behalf of all others similarly situated, allege the following against Progressive Casualty Insurance Company ("Defendant").

NATURE OF THE ACTION

1. Plaintiff brings this class action lawsuit due to Defendant's failure to properly secure and safeguard sensitive and confidential personally identifiable information ("PII")[1], including name, address, driver's license number, email address, phone number, and the date of birth of many of its current customers.[2]

[1] Personally identifiable information generally incorporates information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal oridentifying information. 2 C.F.R. § 200.79. At a minimum, it includes all information that on its face expressly identifies an individual.
[2] *See* Notice of Security Incident, Exhibit A.

2. Defendant's wrongful disclosure has harmed Plaintiff and the Classes (defined below), which include approximately 347,100 people.[3] Many of these people now have their account information accessible by cybercriminals and will be more likely to be victims of cyber-attacks and potential scams.

3. Defendant knew or should have known that due the increasing number of well-publicized data breaches that have occurred in the United States, large data storage such as this require the highest level of protection, which Defendant failed to provide.

4. Plaintiff and members of the Classes ("Class Members") entrusted Defendant with their sensitive and valuable Personal Information. Plaintiff and Class Members did not know that Defendant's data security was inadequate. They did not expect that services offered by Defendant would directly cause such serious injuries that would last for years after the service.

5. Defendant has caused harm to Plaintiff and Class Members by collecting, using, and maintaining their Personal Information for its own economic benefit but utterly failing to protect that information. Defendant did not maintain adequate security systems, did not properly archive Personal Information, allowed access by third parties, and did not implement sufficient security measures.

JURISDICTION AND VENUE

6. This Court possesses subject-matter jurisdiction to adjudicate the claims set forth herein under the provisions of the Class Action Fairness Act ("CAFA"), 28 U.S.C. § 1332(d), because (1) the matter in controversy exceeds the sum or value of $5,000,000, exclusive of interest

[3] https://apps.web.maine.gov/online/aeviewer/ME/40/7832b375-dedf-4be0-9437-1329b9c6a55b.shtml

and costs, (2) the action is a class action, (3) there are members of the Classes, including Plaintiff, who are citizens of States diverse from Defendant, and (4) there are more than 100 Class Members.

7. This Court has Personal Jurisdiction over Defendant because Defendant has sufficient minimal contacts with this District. Defendant has purposefully availed itself to this Jurisdiction through its marketing, sale, advertising, and promotion of its products, services, and retail stores throughout this Jurisdiction.

8. Venue is proper in this Judicial District pursuant to 28 U.S.C. § 1391 because Defendant transacts its business in this District, and a substantial part of the events and/or omissions giving rise to the claims occurred, in part, within this District.

PARTIES

PLAINTIFF

9. Plaintiff Dodie Waden is a resident of Columbia, South Carolina.

10. On August 1, 2023, Plaintiff Waden received notice from Progressive that her personal data had been exposed in Defendant's data breach.

11. Plaintiff Waden has been careful to protect her PII that was exposed in the Defendant's data breach.

12. Plaintiff Waden will continue to be at a higher risk of cyber-attacks, as well as the target of spam and scams for the foreseeable future because of Defendant's breach.

DEFENDANT

13. Defendant Progressive Casualty Insurance Company is an Ohio corporation with its principal place of business located at 6300 Wilson Mills Road, Mayfield Village, Ohio, 44143.

FACTUAL ALLEGATIONS

14. In order to obtain products and/or services from Defendant, Progressive required Plaintiff and the Classes to disclose their highly sensitive Private Information to Progressive.

15. According to a Notice of Security Incident sent to Plaintiff on August 1, 2023, Progressive received written notification from one of their third-party service providers regarding an incident involving some of its call center representatives. Progressive subsequently learned that some of the third-party service provider's employees improperly shared their Progressive access credentials with unauthorized individuals who performed the employees' call center job duties. "This gave the unauthorized individuals access to certain personal information for some of our customers."[4]

16. Most concerningly, "Based on information from the third-party service provider, the earliest date of employment of any of the potentially involved employees by the third-party service provider was May 2021, but most were hired during or after the fall of 2022."[5] This means that unauthorized individuals had unfettered access to Plaintiff's and the Class's Private Information for more than days or weeks, but likely years (May 2021 through May 2023). Progressive gave no indication as to when such unauthorized access stopped.

17. According to disclosures made by Progressive to the Texas Attorney General, the compromised Private Information (or "PII") included sensitive information such as: names, addresses, social security numbers, driver's license numbers, financial information (account numbers, credit card numbers, and/or debit card numbers).[6]

[4] Exhibit A
[5] *Id.*
[6] See https://oag.my.site.com/datasecuritybreachreport/apex/DataSecurityReportsPage.

18. Despite having known about the Data Breach since May 2023, the Notices of Security Incident were not sent to affected individuals until on or around August 1, 2023 – almost three months later.

19. Defendant failed to provide timely notice to Plaintiff and Class Members of the Data Breach.

20. The Private Information accessed in the Data Breach included: first and last names, dates of birth, driver's license numbers, email addresses, and phone numbers.[7]

21. Plaintiff has invested, and will continue in perpetuity to invest, time and money into precautionary measures that could, but may not successfully, mitigate the potential misuse of her data.

22. The Data Breach was the product of an intentional criminal act to gain access to the data. It was the result of a sophisticated, intentional, and malicious attack by professional cybercriminal hackers. Thus, the risk that the victims will experience identity theft or fraud is much more real.

23. By obtaining, collecting, using, and deriving a benefit from Plaintiff's and the Class's Private Information, Defendant assumed legal and equitable duties and knew or should have known that it was responsible for protecting Plaintiff's and the Class's Private Information from unauthorized access and disclosure.

24. As a result of the Data Breach, Plaintiff and members of the Classes have already received a higher volume of phishing emails and spam telephone calls. Such scams trick consumers into giving more information and other valuable personal information to scammers. This

[7] Exhibit A

significantly increases the risk of further substantial damages to Plaintiff and the Classes, including, but not limited to, monetary and identity theft.

25. Despite the risk of future harm to Plaintiff and the Classes, Progressive has only offered two years of credit monitoring and identity theft protection services to Plaintiff and the Classes. This offer is wholly inadequate to protect Plaintiff and the Classes from the lifetime risk of harm they face.

26. Defendant neglected to implement essential precautions to secure and shield the private information of the plaintiff and other class members from unauthorized access. This failure includes a lack of supervision, monitoring, and oversight of third parties hired by the defendant who had access to the Plaintiff's and the Class's personally identifiable information (PII). It was incumbent upon Progressive to guarantee that any third parties it enlisted adhered to sufficient data security procedures, practices, and protocols to prevent unauthorized access.

27. Defendant is no stranger to such security incidents. In 2006, a Progressive employee wrongfully accessed information confidential customer information, including: names, Social Security numbers, dates of birth, and property addresses.[8]

28. Again, in 2015, "Progressive security holes put 2 million at risk", where telematic devices offered by Progressive were noted to have "dozens of security flaws that could be exploited by hackers" and "once compromised, the consequences range from data loss to life and limb."[9]

CLASS ACTION ALLEGATIONS

[8] https://www.computerworld.com/article/2562543/data-breach-at-progressivehighlights-insider-threat.html (last visited Jan. 17, 2024)
[9] https://www.insurancebusinessmag.com/us/news/breaking-news/progressive-security-holes-put-2-million-at-risk-21007.aspx (last visited Jan. 17, 2024)

29. Plaintiff brings this action on behalf of herself, and all others similarly situated pursuant to Rule 23(a) and Rule 23 (b)(3) of the Federal Rules of Civil Procedure. Plaintiff seeks class certification on behalf of the classes defined as follows ("the Classes").

> **Nationwide Class:** All individuals residing in the United States who received a Notice Letter from Progressive informing them that their information may have been compromised in the Data Breach.
>
> **South Carolina Sub Class:** All persons in South Carolina who have received a Notice Letter from Progressive informing them that their information may have been compromised in the Data Breach.

30. Excluded from the Classes are Defendant, any parent companies, subsidiaries, and/or affiliates, officers, directors, legal representatives, employees, co-conspirators, all governmental entities, and any judge, justice or judicial officer presiding over this matter.

31. The Nationwide Class shall and South Carolina Sub Class be referred to as the "Class" or "Classes." Proposed Members of said Class will be referred to as "Class Members," or otherwise referenced as "members of the Class."

32. **Numerosity:** The members of the Classes are so numerous that joinder of all members of the Classes is impracticable. Plaintiff is informed and believe that the proposed Classes contains thousands of customers who have been damaged by Defendant's conduct as alleged herein. The precise number of Class Members is estimated to be 347,100 individuals.

33. **Typicality:** Plaintiff's claims are typical to those of all Class Members because members of the Classes are similarly injured through Defendant's uniform misconduct described above and were subject to their personal data released due to Defendant's conduct. Plaintiff is advancing the same claims and legal theories on behalf of herself and all members of the Classes.

34. **Commonality:** Plaintiff's claims raise questions of law and fact common to all members of the Classes, and they predominate over any questions affecting only individual Class Members. The claims of Plaintiff and all prospective Class Members involve the same alleged data breach. These common legal and factual questions include the following:

a. Whether Defendant's data breach exposed their personal information

b. Whether Defendant owed a duty of care to Plaintiff and the Classes;

c. Whether Defendant knew or should have known that their data security was inadequate;

d. Whether Defendant wrongfully represent, and continue to represent, that their security is adequate;

e. Whether the alleged conduct constitutes violations of the laws asserted;

f. Whether Defendant's alleged conduct violates public policy;

g. Whether Defendant's representations in advertising are false, deceptive, and misleading;

h. Whether a reasonable consumer would consider the risk of their data being exposed when choosing to do business with Defendant;

i. Whether Defendant breached their express warranties;

j. Whether Defendant breached their implied warranties;

k. Whether certification of any or all of the classes proposed herein is appropriate under Fed. R. Civ. P. 23; and

l. Whether Plaintiff and the Class Members are entitled to damages and/or restitution and the proper measure of that loss.

35. **Adequacy:** Plaintiff and her counsel will fairly and adequately protect and represent the interests of each member of the Classes. Plaintiff has retained counsel experienced in complex litigation and class actions. Plaintiff's counsel has successfully litigated other class action cases similar to that here and has the resources and abilities to fully litigate and protect the interests of the Classes. Plaintiff intends to prosecute this claim vigorously. Plaintiff has no adverse or antagonistic interests to those of the Classes, nor is Plaintiff subject to any unique defenses.

36. **Superiority:** A class action is superior to the other available methods for a fair and efficient adjudication of this controversy. The damages or other financial detriment suffered by Plaintiff and the individual Class Members are relatively small compared to the burden and expense that would be entailed by individual litigation of their claims against Defendant. It would thus be virtually impossible for Plaintiff and Class Members, on an individual basis, to obtain meaningful and effective redress for the wrongs done to them. Further, it is desirable to concentrate the litigation of the Class Members' claims in one forum, as it will conserve party and judicial resources and facilitate the consistency of adjudications. Plaintiff knows of no difficulty that would be encountered in the management of this case that would preclude its maintenance as a class action.

37. The Classes also may be certified because Defendant has acted or refused to act on grounds applicable to the Classes, thereby making appropriate final declaratory and/or injunctive relief with respect to the members of the Class as a whole.

38. Plaintiff seeks preliminary and permanent injunctive and equitable relief on behalf of the entire Classes, on grounds generally applicable to the entire Class,es to enjoin and prevent Defendant from continuing to provide inadequate data security. Further, Plaintiff seeks for

Defendant to provide a full refund all protective and defensive procedures that Plaintiff and the Class Members have had to employ.

39. Unless the Classes are certified, Plaintiff and the Class Members will continue to be injured due to Defendant's conduct. Unless a Class-wide injunction is issued, Defendant may continue to commit the violations alleged and the members of the Class and future customers may continue to be placed in harms' way.

CAUSES OF ACTION

COUNT I
NEGLIGENCE
(On Behalf of Plaintiff and the Classes)

40. Plaintiff incorporates Paragraphs 1-39 by reference as if fully set forth herein.

41. As part of the regular course of its business operations Defendant gathered and stored the PII of Plaintiff and Class Members. Plaintiff and the Classes were entirely dependent on Defendant to use reasonable measures to safeguard their PII and were vulnerable to the foreseeable harm of a security breach should Defendant fail to safeguard their PII.

42. By collecting and storing this data in its computer property, and sharing it, and using it for commercial gain, Defendant assumed a duty of care to use reasonable means to secure and safeguard their computer property—and Class Members' PII held within it— to prevent disclosure of the information, and to safeguard the information from theft. Defendant's duty included a responsibility to implement processes by which it could detect a breach of their security systems in a reasonably expeditious period of time and to give prompt notice to those affected in the case of a Data Breach.

43. Defendant owed a duty of care to Plaintiff and the Classes to provide data security consistent with industry standards and other requirements discussed herein, and to ensure that its systems and networks, and the personnel responsible for them, adequately protected the PII.

44. Defendant's duty also arose under Section 5 of the Federal Trade Commission Act ("FTC Act"), 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect PII by companies such as Defendant's. Various FTC publications and data security breach orders further form the basis of Defendant's duty. In addition, individual states have enacted statutes based upon the FTC Act that also created a duty.

45. Plaintiff and the Classes are within the class of persons that the FTC Act was intended to protect.

46. 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 Plaintiff and the Classes.

47. Defendant gathered and stored the PII of Plaintiff and the Classes as part of its business of soliciting its services to its customers which solicitations and services affect commerce.

48. Defendant violated the FTC Act by failing to use reasonable measures to protect the PII of Plaintiff and Class Members and by not complying with applicable industry standards.

49. Defendant breached its duty to Plaintiff and the Classes under the FTC Act by failing to provide fair, reasonable, or adequate computer systems and/or data security practices to safeguard their PII, and by failing to provide prompt notice without reasonable delay.

50. Defendant's duty of care to use reasonable security measures arose as a result of the special relationship that existed between Defendant and its customers, which is recognized by laws and regulations including but not limited to FTCA, as well as common law. Defendant was in a position to ensure that its systems were sufficient to protect against the foreseeable risk of harm to Plaintiff and the Classes or minimize the Data Breach.

51. Defendant's multiple failures to comply with applicable laws and regulations, and the violation of Section of 5 of the FTC Act constitutes negligence *per se*.

52. Defendant's duty to use reasonable care in protecting confidential data arose not only as a result of the statutes and regulations described above, but also because Defendant is bound by industry standards to protect confidential PII.

53. Defendant had full knowledge of the sensitivity of the PII, the types of harm that Plaintiff could and would suffer if the PII was wrongfully disclosed, and the importance of adequate security.

54. Plaintiff and the Class Members were the foreseeable victims of any inadequate safety and security practices. Plaintiff and the Classes had no ability to protect their PII that was in Defendant's possession.

55. Defendant was in a special relationship with Plaintiff and the Classes with respect to the hacked PII because the aim of Defendant's data security measures was to benefit Plaintiff by ensuring that their PII would remain protected and secure. Only Defendant was able to ensure that its systems were sufficiently secure to protect Plaintiff's and other Class Members' PII. The harm to Plaintiff and the Classes from its exposure was highly foreseeable to Defendant.

56. Defendant owed Plaintiff and other Class Members a common law duty to use reasonable care to avoid causing foreseeable risk of harm to Plaintiff and the Classes when

obtaining, storing, using, and managing their PII, including acting to reasonably safeguard such data and providing notification to Plaintiff and the Classes of any breach in a timely manner so that appropriate action could be taken to minimize losses.

57. Defendant had duties to protect and safeguard the PII of Plaintiff and other Class Members from being vulnerable to compromise by taking common-sense precautions when dealing with highly sensitive PII. Additional duties that Defendant owed Plaintiff and the Classes include:

a. Exercising reasonable care in designing, implementing, maintaining, monitoring, and testing Defendant's networks, systems, protocols, policies, procedures, and practices to ensure that individuals PII was adequately secured from impermissible release, disclosure, and publication;
b. To protect Plaintiff's and the Class' PII in its possession by using reasonable and adequate security procedures and systems; and
c. To promptly notify Plaintiff and the Classes of any breach, security incident, unauthorized disclosure, or intrusion that affected or may have affected their PII.

58. Only Defendant was in a position to ensure that its systems and protocols were sufficient to protect the PII that had been entrusted to them.

59. Defendant breached its duty of care by failing to adequately protect Plaintiff's and the Class's PII. Defendant breached their duties by:

a. Failing to exercise reasonable care in obtaining, retaining, securing, safeguarding, protecting, and deleting the PII in its possession;
b. Failing to protect the PII in its possession using reasonable and adequate security procedures and systems;

c. Failing to adequately and properly audit, test, and train its employees regarding how to properly and securely transmit and store PII;

d. Failing to adequately train its employees to not store unencrypted PII in their personal files longer than absolutely necessary for the specific purpose that it was sent or received;

e. Failing to consistently enforce security policies aimed at protecting Plaintiff's and the Class's PII;

f. Failing to mitigate the harm caused to Plaintiff and the Classes;

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

h. Failing to promptly notify Plaintiff's and other Class Members of the Data Breach that affected their PII.

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

61. Defendant, through its actions and/or omissions, unlawfully breached its duty to Plaintiff and the Classes by failing to implement industry protocols and exercise reasonable care in protecting and safeguarding the PII of Plaintiff and the Classes during the time the PII was within Defendant's possession or control.

62. Defendant's failure to provide timely and clear notification of the Data Breach to Plaintiff and the Class prevented Plaintiff and the Classes from taking meaningful, proactive steps to securing their PII and mitigating damages.

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

64. As a direct and proximate result of Defendant's negligence and negligence *per se*, Plaintiff and the Classes 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 actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from tax fraud and identity theft; (vi) costs associated with placing freezes on credit reports; (vii) the continued risk to their PII, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII in their continued possession; and (viii) future costs in terms of time, effort, and money that will be expended to monitor bank accounts and credit reports, 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 Plaintiff and members of the Classes.

65. As a direct and proximate result of Defendant's negligence, Plaintiff, and members of 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.

66. Additionally, as a direct and proximate result of Defendant's negligence and negligence *per se*, Plaintiff and members of the Classes 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 its continued possession.

67. Plaintiff and members of the Classes have suffered injury and are entitled to actual damages in amounts to be proven at trial.

COUNT II
BREACH OF CONTRACT
(On Behalf of Plaintiff and the Classes)

68. Plaintiff incorporates Paragraphs 1-39 by reference as if fully set forth herein.

69. As part of doing business with Defendant, Plaintiff and members of the Classes are required to provide Defendant with personal information when entering a contract with Defendant before they are able to receive the benefit of any services from Defendant.

70. Plaintiff and Class Members were customers of Defendant, and therefore had entered a contract with Defendant.

71. Part of that contract, whether expressed or implied, is that Defendant would provide adequate protection of customer's account and person information, and prevent that data from being given away, sold, or stolen.

72. By failing to adequately update their protection software, Defendant has breached its contracts with Plaintiff and Class Member by proving inadequate protection.

73. This breach has resulted in damages and injuries to all Plaintiff and Class Members, who have had their personal information and account details stolen and thus are more likely to be subject to cyber-attacks, identity fraud, as well as unwanted spam and scam messages.

74. Throughout most of Defendant's history it has provided reasonably proactive data security, preventing many of the cyber-attacks that have targeted Defendant.

75. Defendant's failure to keep and secure the Plaintiff's and Class Members' data constitutes a material breach of the agreements between Defendant and the Plaintiff and Class Members. By doing so, Defendant have harmed each and every Plaintiff and Class Member.

COUNT III
UNJUST ENRICHMENT
(Alternatively, On Behalf of the Plaintiff and the Classes)

76. Plaintiff incorporates Paragraphs 1-39 by reference as if fully set forth herein.

77. Plaintiff and members of the Classes have conferred a benefit to Defendant in the form of monies paid for providing insurance services, a portion of which was intended to have been used by Progressive to ensure that any vendors it hired implemented appropriate data security measures and implemented appropriate user controls.

78. Included in these services provided, whether expressed or implied, is the secured protection and safekeeping of Plaintiff's and Class Members' personal and account information.

79. These monies were not given as a gift, but rather with the expectation and understanding that services would be provided in return.

80. Defendant has accepted and appreciated the monies paid, as it has continued to provide its services to Plaintiff and the Class Members, per the terms of their agreements.

81. Then, in May of 2023, Defendant was no longer able to provide safe and secure protection of Plaintiff's and Class Members' data.

82. This is evident as over 347,100 customers' data was unintentionally released and has been accessed by cybercriminals.

83. Defendant has retained all monies paid by Plaintiff and Class Members, even though they have failed to provide the secure service that Plaintiff and Class Members, whether expressed or implied, paid for.

84. If Plaintiff and Class Members knew that Defendant had given their Private Information to a third-party with virtually no data security measures in place, they would not have agreed to allow Defendant to have or maintain their Private Information.

85. Defendant's retention of these monies paid would be inequitable, as the Plaintiff and Class Members have paid value for a benefit that they were not provided.

86. Not only were the Plaintiff and Class Members not provided a service for which they paid for, but they will now have to pay additional costs out of pocket in attempts of preventing their data from causing them further harm.

87. Plaintiff and Class Members have no adequate remedy at law.

88. As a direct and proximate result of Defendant's decision to profit rather than hire a third-party with adequate data security measures in place, Plaintiff and Class Members have suffered and continue to suffer actual damages, including (i) the amount of the savings and costs Defendant reasonably should have expended to provide a third-party with adequate data security measures to secure Plaintiff's Private Information, (ii) time and expenses mitigating harms, (iii) diminished value of the Private Information, (iv) harms as a result of identity theft; and (v) an increased risk of future identity theft.

COUNT IV
Declaratory Judgment
(On Behalf of the Plaintiff and the Classes)

89. Plaintiff re-alleges and incorporates by reference the paragraphs above as if fully set forth herein.

90. Under the Declaratory Judgment Act, 28 U.S.C. §§ 2201, et seq., this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and grant

further necessary relief. Furthermore, the Court has broad authority to restrain acts, such as here, that are tortious and violate the terms of the federal and state statutes described in this Complaint.

91. An actual controversy has arisen in the wake of Defendant's data breach regarding its present and prospective common law and other duties to reasonably safeguard its customers' PII and whether Defendant is currently maintaining data security measures adequate to protect Plaintiff from further data breaches that compromise their PII.

92. Plaintiff alleges that Defendant's data security measures remain inadequate. Plaintiff will continue to suffer injury as a result of the compromise of their PII and remain at imminent risk that further compromises of their PII will occur in the future.

93. Pursuant to its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following: (i) Defendant continues to owe a legal duty to secure current and former employees' PII and to timely notify employees and former employees of a data breach under the common law, Section 5 of the FTC Act, and various state statutes; (ii) Defendant continues to breach this legal duty by failing to employ reasonable measures to secure Plaintiff's and Class Members' PII.

94. The Court also should issue corresponding prospective injunctive relief requiring that Defendant employ adequate security protocols consistent with law and industry standards to protect consumers' PII.

95. If an injunction is not issued, Plaintiff will suffer irreparable injury, and lack an adequate legal remedy, in the event of another data breach targeted at Defendant. The risk of another such breach is real, immediate, and substantial. If another breach targeted at Defendant occurs, Plaintiff will not have an adequate remedy at law because many of the resulting injuries

are not readily quantified and they will be forced to bring multiple lawsuits to rectify the same conduct.

96. The hardship to Plaintiff if an injunction does not issue exceeds the hardship to Defendant if an injunction is issued. Among other things, if another massive data breach occurs which is targeted at Defendant, Plaintiff will likely be subjected to fraud, identify theft, and other harms described herein. On the other hand, the cost of complying with an injunction by employing reasonable prospective data security measures is relatively minimal, and Defendant has a pre-existing legal obligation to employ such measures.

97. Issuance of the requested injunction will not do a disservice to the public interest. To the contrary, such an injunction would benefit the public by preventing another data breach at Defendant, thus eliminating the additional injuries that would result to Plaintiff and the millions of individuals whose PII would be further compromised.

PRAYER FOR RELIEF

Plaintiff, individually and on behalf of the Classes, respectfully request the Court to enter judgment on her behalf and on behalf of the Classes as follows:

a) Certification of the action as a Class Action Pursuant to Federal Rule of Civil Procedure 23, and appointment of Plaintiff as Class Representatives and her counsel of record as Class Counsel;

b) That acts alleged herein be adjudged and decreed to constitute negligence, breach of contract, and unjust enrichment.

c) A judgment against Defendant for the damages sustained by Plaintiff and the Classes defined herein, and for any additional damages, penalties, and other monetary relief provided by applicable law;

d) An order providing injunctive and other equitable relief as necessary to protect the interests of the Classes, including, but not limited to:

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

(2) Ordering that Defendant engage third-party security auditors and internal personnel to run automated security monitoring;

(3) Ordering that Defendant audits, tests, and trains its security personnel regarding any new or modified procedures;

(4) Ordering that Defendant segment consumer data by, among other things, creating firewalls and access controls so that if one area of Defendant's systems is compromised, unauthorized third parties cannot gain access to other portions of Defendant's systems;

(5) Ordering that Defendant purge, delete, and destroy in a reasonably secure manner consumer data not necessary for its provisions of services;

(6) Ordering that Defendant conducts regular database scanning; and

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

e) By awarding Plaintiff and Class Members pre-judgment and post-judgment interest as provided by law, and that such interest be awarded at the highest legal rate from and after the date of service of the Complaint in this action;

f) The costs of this suit, including reasonable attorney fees; and

g) Such other and further relief as the Court deems just and proper.

DEMAND FOR JURY TRIAL

Plaintiff, individually and on behalf of all those similarly situated, hereby requests a jury trial, pursuant to Federal Rule of Civil Procedure 38, on any and all claims so triable.

Dated: January 17, 2024

/s/Blake G. Abbott
Paul J. Doolittle (Fed ID #6012)
Blake G. Abbott (Fed ID #13354)
POULIN | WILLEY | ANASTOPOULO, LLC
32 Ann Street
Charleston, SC 29403
Tel: (803) 222-2222
Email: paul.doolittle@poulinwilley.com
blake.abbott@poulinwilley.com

Attorneys for Plaintiff