THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF NEW YORK

ANDRE SAMUEL HAMID

and

AMY LYNN HAMID,

on behalf of themselves and all others similarly situated,

Plaintiffs,

vs.

CANON, U.S.A., INC.,
a New York corporation,

CANON SOLUTIONS AMERICA, INC.,
a New York corporation,

CANON SOFTWARE AMERICA, INC.,
a New York corporation,

CANON INFORMATION AND IMAGING SOLUTIONS, INC.,
a New York corporation,

CANON FINANCIAL SERVICES, INC.,
a New Jersey corporation,

CANON MEDICAL COMPONENTS U.S.A, INC.,
a California corporation,

CANON INFORMATION TECHNOLOGY SERVICES, INC.,
a Virginia corporation,

and

NT-WARE USA, INC.,
a Delaware corporation,

Defendants.

Case No.:

CLASS ACTION COMPLAINT

DEMAND FOR JURY TRIAL

Plaintiffs Andre Samuel Hamid and Amy Lynn Hamid ("Plaintiffs") bring this Amended Class Action Complaint against Canon U.S.A., Inc., Canon Solutions America, Inc., Canon Software America, Inc., Canon Information and Imaging Solutions, Inc., Canon Financial Services, Inc., Canon Medical Components U.S.A., Inc., Canon Information Technology Services, Inc., and NT-ware USA, Inc. (collectively, "Canon" or "Defendants"), as individuals and on behalf of all others similarly situated, and allege, upon personal knowledge as to their own actions and their counsels' investigations, and upon information and belief as to all other matters, as follows:

I. INTRODUCTION

1. Plaintiffs bring this class action against Defendants for their failure to properly secure and safeguard personal identifiable information that Defendants required from their employees as a condition of employment, including without limitation, names, Social Security numbers, driver's license numbers or government-issued identification numbers, financial account numbers provided for direct deposit, electronic signatures, and dates of birth (collectively, "personal identifiable information" or "PII"). Plaintiffs also allege Defendants failed to provide timely, accurate, and adequate notice to Plaintiffs and similarly situated current and former employees and their beneficiaries and dependents (collectively, "Class Members") that their PII had been lost and precisely what types of information was unencrypted and in the possession of unknown third parties.

2. Defendants are a leading provider of consumer, business-to-business, and industrial digital imaging solutions to the United States and to Latin American and the Caribbean markets. Defendants' employees entrust Defendants with an extensive amount of PII. Defendants retain this information on computer hardware—even after the employment relationship ends. Defendants assert that they understand the importance of protecting information.

3. On or before August 4, 2020, Defendants learned that a data breach had occurred and that it involved ransomware).

4. Defendants determined that the Data Breach involved unauthorized activity on their network between July 20, 2020 and August 6, 2020, including unauthorized access to files on Defendants' servers (the "Data Breach"). These servers contained files that in turn contained information about current and former employees and their beneficiaries and dependents.

5. On or around August 6, 2020, Defendants circulated an internal alert to their employees disclosing the Data Breach.

6. In a "Notice of Data Breach," dated November 24, 2020, Defendants advised that they were informing current and former employees of Defendants from 2005 to 2020, and their beneficiaries and dependents, of the data breach incident.

7. By obtaining, collecting, using, and deriving a benefit from Plaintiffs' and Class Members' PII, Defendants assumed legal and equitable duties to those individuals. Defendants admit that the unencrypted PII exposed to "unauthorized activity" included names, Social Security numbers, driver's license numbers or government-issued identification numbers, financial account numbers provided for direct deposit, electronic signatures, and dates of birth.

8. The exposed PII of Defendants' current and former employees and their beneficiaries and dependents can be sold on the dark web. Hackers can access and then offer for sale the unencrypted, unredacted PII to criminals. Defendants' current and former employees and their beneficiaries and dependents face a lifetime risk of identity theft, which is heightened here by the loss of Social Security numbers and electronic signatures.

9. This PII was compromised due to Defendants' negligent and/or careless acts and omissions and the failure to protect PII of their current and former employees and their

beneficiaries and dependents. In addition to Defendants' failure to prevent the Data Breach, after discovering the breach, Defendants waited several months to report it to the states' Attorneys General and affected individuals.

10. As a result of this delayed response, Plaintiffs and Class Members had no idea their PII had been compromised, and that they were, and continue to be, at significant risk to identity theft and various other forms of personal, social, and financial harm. The risk will remain for their respective lifetimes.

11. Plaintiffs bring this action on behalf of all persons whose PII was compromised as a result of Defendants' failure to: (i) adequately protect the PII of their current and former employees and their beneficiaries and dependents; (ii) warn their current and former employees and their beneficiaries and dependents of their inadequate information security practices; and (iii) effectively secure hardware containing protected PII using reasonable and effective security procedures free of vulnerabilities and incidents. Defendants' conduct amounts to negligence and violates federal and state statutes.

12. Plaintiffs and Class Members have suffered injury as a result of Defendants' conduct. These injuries include: (i) lost or diminished value of PII; (ii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII; (iii) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, including but not limited to lost time, and (iv) the continued and certainly an increased risk to their PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) may remain backed up in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fails to undertake appropriate and adequate measures to protect the PII.

13. Defendants disregarded the rights of Plaintiffs and Class Members by intentionally, willfully, recklessly, or negligently failing to take and implement adequate and reasonable measures to ensure that their current and former employees' PII, and that of their beneficiaries and dependents, was safeguarded, failing to take available steps to prevent an unauthorized disclosure of data, and failing to follow applicable, required and appropriate protocols, policies and procedures regarding the encryption of data, even for internal use. As the result, the PII of Plaintiffs and Class Members was compromised through disclosure to an unknown and unauthorized third party. Plaintiffs and Class Members have a continuing interest in ensuring that their information is and remains safe, and they should be entitled to injunctive and other equitable relief.

II. PARTIES

14. Plaintiff Andre Samuel Hamid is a Citizen of Colorado residing in Larimer County, Colorado. Mr. Hamid received Canon's *Notice of Data Breach*, dated November 24, 2020, on or about that date.

15. Plaintiff Amy Lynn Hamid is a Citizen of Colorado residing in Larimer County, Colorado. Ms. Hamid received Canon's *Notice of Data Breach*, dated November 24, 2020, on or about that date.

16. Defendant Canon U.S.A., Inc. is a corporation organized under the laws of New York, headquartered at One Canon Park, Melville, New York, with its principal place of business in Melville, New York.

17. Defendant Canon Solutions America, Inc. is a corporation organized under the laws of New York, headquartered at One Canon Park, Melville, New York, with its principal place of business in Melville, New York.

18. Defendant Canon Software America, Inc. is a corporation organized under the laws

of New York, headquartered at One Canon Park, Melville, New York, with its principal place of business in Melville, New York.

19. Defendant Canon Information and Imaging Solutions, Inc. is a corporation organized under the laws of New York, headquartered at One Canon Park, Melville, New York, with its principal place of business in Melville, New York.

20. Defendant Canon Financial Services, Inc. is a corporation organized under the laws of New Jersey, headquartered at 158 Gaither Drive, Mt. Laurel, New Jersey, with its principal place of business in Mt. Laurel, New Jersey.

21. Defendant Canon Medical Components U.S.A., Inc. is a corporation organized under the laws of California, headquartered at 15955 Alton Parkway, Irvine, California, with its principal place of business in Irvine, California.

22. Defendant Canon Information Technology Services, Inc. is a corporation organized under the laws of Virginia, headquartered at 850 K Greenbrier Circle, Chesapeake, Virginia with its principal place of business in Chesapeake, Virginia.

23. Defendant NT-ware USA, Inc. is a corporation organized under the laws of Delaware, headquartered at 105 Maxess Road, Suite S129, Melville, New York, with its principal place of business in Melville, New York.

24. The true names and capacities of persons or entities, whether individual, corporate, associate, or otherwise, who may be responsible for some of the claims alleged herein are currently unknown to Plaintiffs. Plaintiffs will seek leave of court to amend this complaint to reflect the true names and capacities of such other responsible parties when their identities become known.

25. All of Plaintiffs' claims stated herein are asserted against Defendants and any of their owners, predecessors, successors, subsidiaries, agents and/or assigns.

III. JURISDICTION AND VENUE

26. This Court has subject matter and diversity jurisdiction over this action under 28 U.S.C. § 1332(d) because this is a class action wherein the amount of controversy exceeds the sum or value of $5 million, exclusive of interest and costs, there are more than 100 members in the proposed class, and at least one other Class Member (including named Plaintiff Andrew Samuel Hamid, a Citizen of Colorado) is a citizen of a state different from Defendants to establish minimal diversity.

27. The Eastern District of New York has personal jurisdiction over Defendants named in this action because Defendants and/or their parents or affiliates are headquartered in this District and Defendants conduct substantial business in New York and this District through their headquarters, offices, parents, and affiliates.

28. Venue is proper in this District under 28 U.S.C. §1391(b) because Defendants and/or their parents or affiliates are headquartered in this District and a substantial part of the events or omissions giving rise to Plaintiffs' claims occurred in this District.

IV. FACTUAL ALLEGATIONS

Background

29. Defendants are a leading provider of consumer, business-to-business, and industrial digital imaging solutions to the United States and to Latin America and the Caribbean markets with multiple subsidiaries, predecessors, and affiliates and more than 18,000 employees.

30. Plaintiffs and Class Members employed by Defendants were required to provide some of their most sensitive and confidential information for themselves and their beneficiaries and dependents, including names, dates of birth, Social Security numbers, electronic signatures, and other personal identifiable information which is static, does not change, and can be used to

commit myriad financial crimes.

31. Plaintiffs and Class Members, as current and former employees and their beneficiaries and dependents, relied on these sophisticated Defendants to keep their PII confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information. Defendants' current and former employees and their beneficiaries and dependents demand security to safeguard their PII.

32. Defendants had a duty to adopt reasonable measures to protect Plaintiffs' and Class Members' PII from involuntary disclosure to third parties.

The Data Breach

33. Beginning on or about November 24, 2020, Defendants sent their current and former employees and their beneficiaries and dependents a *Notice of Data Breach*.[1] Defendants informed the recipients of the notice that:

> We identified a security incident involving ransomware on August 4, 2020. We immediately began to investigate, a cybersecurity firm was engaged, and measures were taken to address the incident and restore operations. We also notified law enforcement and worked to support the investigation. We determined that there was unauthorized activity on our network between July 20, 2020 and August 6, 2020. During that time, there was unauthorized access to files on our file servers.
>
> We completed a careful review of the file servers on November 2, 2020 and determined that there were files that contained information about current and former employees from 2005 to 2020 and their beneficiaries and dependents. The information in the files included the individuals' names and one or more of the following data elements: Social Security number, driver's license number or government-issued identification number, financial account number provided to Canon for direct deposit, electronic signature, and date of birth.[2]

[1] *See Notice of Data Breach*, available at https://cfs.canon.com/SecurityIncident-CA.html, a true and correct copy of which is attached hereto as Exhibit 1 ("Ex. 1").
[2] Ex. 1, p.1.

34. On or about November 25, 2020, Defendants sent data breach notifications to various state Attorneys General, including Vermont's Attorney General TJ Donovan, signed by N. Scott Millar, Defendant Canon U.S.A., Inc.'s Senior Vice President & General Manager.[3]

35. Defendants admitted in the *Notice of Data Breach* and the letters to the Attorneys General that unauthorized third persons accessed files that contained sensitive information about current and former employees and their beneficiaries and dependents, including names, social security numbers, driver's license numbers or government-issues identification numbers, financial accounts numbers provided to Defendants for direct deposit, electronic signatures, and dates of birth.

36. In response to the Data Breach, Defendants claim that they "immediately began to investigate, a cybersecurity firm was engaged, and measures were taken to address the incident and restore operations. We notified law enforcement and worked to support the investigation. We also implemented additional security measures to further enhance the security of our network."[4]

37. Plaintiffs' and Class Members' unencrypted information may end up for sale on the dark web, or simply fall into the hands of companies that will use the detailed PII for targeted marketing without the approval of the affected current and former employees and their beneficiaries and dependents. Unauthorized individuals can easily access the PII of Defendants' current and former employees and their beneficiaries and dependents.

38. Defendants did not use reasonable security procedures and practices appropriate to the nature of the sensitive, unencrypted information they were maintaining for current and former employees and their beneficiaries and dependents, causing Plaintiffs' and Class Members' PII to be exposed.

[3] Ex. 2.
[4] Exs. 1, 2.

Defendants' Acquire, Collect and Store Plaintiffs' and Class Members' PII.

39. Defendants acquired, collected, and stored their current and former employees' PII, and that of their beneficiaries and dependents, at least from 2005 to 2020.

40. As a condition of maintaining employment with Defendants, Defendants require that their employees entrust Defendants with highly confidential PII.

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

42. Plaintiffs and the Class Members have taken reasonable steps to maintain the confidentiality of their PII. Plaintiffs and the Class Members, as current and former employees and their beneficiaries and dependents, relied on Defendants to keep their PII confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information.

Securing PII and Preventing Breaches

43. Defendants could have prevented this Data Breach by properly securing and encrypting the files and file servers containing Plaintiffs' and Class Members' PII. Or Defendants could have destroyed the data, especially decade-old data from former employees and their beneficiaries and dependents.

44. Defendants' negligence in safeguarding their current and former employees' PII, and that of their beneficiaries and dependents, is exacerbated by the repeated warnings and alerts directed to protecting and securing sensitive data.

45. Despite the prevalence of public announcements of data breach and data security compromises, Defendants failed to take appropriate steps to protect the PII of Plaintiffs and the

proposed Class from being compromised.

46. The Federal Trade Commission ("FTC") defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority."[5] 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."[6]

47. The ramifications of Defendants' failure to keep secure their current and former employees' PII, and that of their beneficiaries and dependents, are long lasting and severe. Once PII is stolen, particularly Social Security numbers, fraudulent use of that information and damage to victims may continue for years.

Value of Personal Identifiable Information

48. 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.[7] Experian reports that a stolen credit or debit card number can sell for $5 to $110 on the dark web.[8] Criminals can also purchase access to entire

[5] 17 C.F.R. § 248.201 (2013).
[6] *Id.*
[7] *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 Dec. 30, 2020).
[8] *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 Dec. 29, 2020).

company data breaches from $900 to $4,500.[9]

49. Social Security numbers, for example, are among the worst kind of personal information to have stolen because they may be put to a variety of fraudulent uses and are difficult for an individual to change. The Social Security Administration stresses that the loss of an individual's Social Security number, as is the case here, can lead to identity theft and extensive financial fraud:

> A dishonest person who has your Social Security number can use it to get other personal information about you. Identity thieves can use your number and your good credit to apply for more credit in your name. Then, they use the credit cards and don't pay the bills, it damages your credit. You may not find out that someone is using your number until you're turned down for credit, or you begin to get calls from unknown creditors demanding payment for items you never bought. Someone illegally using your Social Security number and assuming your identity can cause a lot of problems.[10]

50. What is more, it is no easy task to change or cancel a stolen Social Security number. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. In other words, preventive action to defend against the possibility of misuse of a Social Security number is not permitted; an individual must show evidence of actual, ongoing fraud activity to obtain a new number.

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

---

[9] *In the Dark*, VPNOverview, 2019, *available at*: https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/ (last accessedDec. 29, 2020).

[10] Social Security Administration, *Identity Theft and Your Social Security Number*, *available at*: https://www.ssa.gov/pubs/EN-05-10064.pdf (last accessed Dec. 29, 2020).

into the new Social Security number."[11]

52. Based on the foregoing, the information compromised in the Data Breach is significantly more valuable than the loss of, for example, credit card information in a retailer data breach, because, there, victims can cancel or close credit and debit card accounts. The information compromised in this Data Breach is impossible to "close" and difficult, if not impossible, to change—Social Security number, driver's license number or government-issued identification number, name, and date of birth.

53. This data demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "Compared to credit card information, personally identifiable information and Social Security numbers are worth more than 10x on the black market."[12]

54. Among other forms of fraud, identity thieves may obtain driver's licenses, government benefits, medical services, and housing or even give false information to police.

55. The fraudulent activity resulting from the Data Breach may not come to light for years.

56. 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

[11] Bryan Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR (Feb. 9, 2015), *available at*: http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millionsworrying-about-identity-theft (last accessed Dec. 29, 2020).

[12] Time Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, IT World, (Feb. 6, 2015), *available at*: https://www.networkworld.com/article/2880366/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html (last accessed Dec. 29, 2020).

> 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.[13]

57. At all relevant times, Defendants knew, or reasonably should have known, of the importance of safeguarding their current and former employees' PII, and that of their beneficiaries and dependents, including Social Security numbers and dates of birth, and of the foreseeable consequences that would occur if Defendants' data security system was breached, including, specifically, the significant costs that would be imposed on Defendants' current and former employees and their beneficiaries and dependents as a result of a breach.

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

59. Defendants were, or should have been, fully aware of the unique type and the significant volume of data on Defendants' file servers, amounting to potentially tens or hundreds of thousands of individuals' detailed, personal information and thus, the significant number of individuals who would be harmed by the exposure of the unencrypted data.

60. To date, Defendants have offered their current and former employees and their beneficiaries and dependents only one year of credit monitoring service through a single credit bureau, Experian. The offered service is inadequate to protect Plaintiffs and Class Members from the threats they face for years to come, particularly in light of the PII at issue here.

61. 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

[13] *Report to Congressional Requesters*, GAO, at 29 (June 2007), *available at:* http://www.gao.gov/new.items/d07737.pdf (last accessed Dec. 29, 2020).

their current and former employees and their beneficiaries and dependents.

Plaintiff Andre Samuel Hamid's Experience

62. From in or about May 2019 to June 2020, Plaintiff Andre Hamid worked for Defendant Canon Solutions America, Inc. in Centennial, Colorado. As a condition of employment, Defendants required that he provide his PII, including but not limited to his name, address, driver's license number, financial account information, bank account numbers, date of birth, electronic signature, and Social Security number.

63. Mr. Hamid received the Notice of Data Breach, dated November 24, 2020, on or about that date.

64. As a result of the Data Breach notice, Mr. Hamid spent time dealing with the consequences of the Data Breach, which includes time spent verifying the legitimacy of the Notice of Data Breach, exploring credit monitoring and identity theft insurance options, signing up and routinely monitoring the credit monitoring offered by Defendants, and self-monitoring his accounts. This time has been lost forever and cannot be recaptured.

65. Additionally, Mr. Hamid is very careful about sharing his PII. He has never knowingly transmitted unencrypted PII over the internet or any other unsecured source.

66. Mr. Hamid stores any documents containing his PII in a safe and secure location, or destroys the documents. Moreover, he diligently chooses unique usernames and passwords for his various online accounts.

67. Mr. Hamid suffered actual injury in the form of damages to and diminution in the value of his PII—a form of intangible property that Mr. Hamid entrusted to Defendants for the purpose of his employment, which was compromised in and as a result of the Data Breach.

68. Mr. Hamid suffered lost time, annoyance, interference, and inconvenience as a

result of the Data Breach and has anxiety and increased concerns for the loss of his privacy.

69. Mr. Hamid has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from his PII, especially his Social Security number, in combination with his name, driver's license and electronic signature, being placed in the hands of unauthorized third-parties and possibly criminals.

70. Mr. Hamid has a continuing interest in ensuring that his PII, which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future breaches.

Plaintiff Amy Lynn Hamid's Experience

71. From in or about May 2019 to June 2020, Plaintiff Amy Lynn Hamid's husband, Plaintiff Andre Hamid, worked for Defendant Canon Solutions America, Inc. in Centennial, Colorado. As a condition of his employment, Defendants required that he provide Ms. Hamid's PII, including but not limited to her name, address, driver's license number, financial account information, bank account numbers, date of birth, and Social Security number.

72. Ms. Hamid received the Notice of Data Breach, dated November 24, 2020, on or about that date.

73. As a result of the Data Breach notice, Ms. Hamid spent time dealing with the consequences of the Data Breach, which includes time spent verifying the legitimacy of the Notice of Data Breach, exploring credit monitoring and identity theft insurance options, signing up and routinely monitoring the credit monitoring offered by Defendants, and self-monitoring her accounts. This time has been lost forever and cannot be recaptured.

74. Additionally, Ms. Hamid is very careful about sharing her PII. She has never knowingly transmitted unencrypted PII over the internet or any other unsecured source.

75. Ms. Hamid stores any documents containing her PII in a safe and secure location, or destroys the documents. Moreover, she diligently chooses unique usernames and passwords for his various online accounts.

76. Ms. Hamid suffered actual injury in the form of damages to and diminution in the value of her PII—a form of intangible property that Ms. Hamid entrusted to Defendants for the purpose of her husband's employment, which was compromised in and as a result of the Data Breach.

77. Ms. Hamid suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach and has anxiety and increased concerns for the loss of his privacy.

78. Ms. Hamid has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from his PII, especially her Social Security number, in combination with her name, driver's license and electronic signature, being placed in the hands of unauthorized third-parties and possibly criminals.

79. Ms. Hamid has a continuing interest in ensuring that her PII, which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future breaches.

V. CLASS ALLEGATIONS

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

81. The Nationwide Class that Plaintiffs seek to represent is defined as follows:

> All individuals whose PII was compromised in the data breach first announced by Defendants on or about November 24, 2020 (the "Nationwide Class").

82. Pursuant to Rule 23, and in the alternative to claims asserted on behalf of the Nationwide Class, Plaintiff Andre Samuel Hamid asserts claims on behalf of a separate statewide subclass, defined as follows:

> All current and former employees of any of Defendants who had contracts with any of Defendants related to PII that was compromised in the data breach first announced by Defendants on or about November 24, 2020 (the "Contracted Employees Subclass").

83. Pursuant to Rule 23, and in the alternative to claims asserted on behalf of the Nationwide Class, Plaintiff Amy Lynn Hamid asserts claims on behalf of a separate statewide subclass, defined as follows:

> All beneficiaries and dependents of any current or former employees of any of Defendants who had contracts with any of Defendants related to PII that was compromised in the data breach first announced by Defendants on or about November 24, 2020 (the "Third-Party Beneficiaries Subclass").

84. Excluded from the Classes are the following individuals and/or entities: Defendants and Defendants' parents, subsidiaries, affiliates, officers and directors, current or former employees, and any entity in which Defendants 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.

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

86. Numerosity, Fed R. Civ. P. 23(a)(1): The Nationwide Class (the "Class") are so numerous that joinder of all members is impracticable. Defendants have identified thousands of

current and former employees, and beneficiaries and dependents thereof, whose PII may have been improperly accessed in the Data Breach, and the Class is apparently identifiable within Defendants' records.

87. 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 Defendants had a duty to protect the PII of Plaintiffs and Class Members;

b. Whether Defendants had respective duties not to disclose the PII of Plaintiffs and Class Members to unauthorized third parties;

c. Whether Defendants had respective duties not to use the PII of Plaintiffs and Class Members for non-business purposes;

d. Whether Defendants failed to adequately safeguard the PII of Plaintiffs and Class Members;

e. Whether and when Defendants actually learned of the Data Breach;

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

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

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

i. Whether Defendants adequately addressed and fixed the vulnerabilities which

permitted the Data Breach to occur;

j. Whether Defendants engaged in unfair, unlawful, or deceptive practices by failing to safeguard the PII of Plaintiffs and Class Members;

k. Whether Plaintiffs and Class Members are entitled to actual, damages, statutory damages, and/or punitive damages as a result of Defendants' wrongful conduct;

l. Whether Plaintiffs and Class Members are entitled to restitution as a result of Defendants' wrongful conduct; and

m. 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.

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

89. Policies Generally Applicable to the Class: This class action is also appropriate for certification because Defendants 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. Defendants' policies challenged herein apply to and affect Class Members uniformly and Plaintiffs' challenge of these policies hinges on Defendants' conduct with respect to the Class as a whole, not on facts or law applicable only to Plaintiffs.

90. Adequacy, Fed. R. Civ. P. 23(a)(4): Plaintiffs will fairly and adequately represent and protect the interests of the Class Members in that they 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 they have suffered are typical of other Class Members. Plaintiffs have retained counsel experienced in complex class action litigation, and Plaintiffs intend to prosecute this action vigorously.

91. Superiority and Manageability, Fed. R. Civ. P. 23(b)(3): The 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 Defendants. 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.

92. 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 Defendants 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.

93. The litigation of the claims brought herein is manageable. Defendants' 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.

94. Adequate notice can be given to Class Members directly using information maintained in Defendants' records.

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

96. Further, Defendants 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.

97. 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 Defendants owed a legal duty to Plaintiffs and Class Members to exercise due care in collecting, storing, using, and safeguarding their PII;

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

c. Whether Defendants 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 Defendants on the one hand, and Plaintiffs and Class Members on the other, and the terms of that implied contract;

e. Whether Defendants breached the implied contract;

f. Whether Defendants adequately, and accurately informed Plaintiffs and Class Members that their PII had been compromised;

g. Whether Defendants 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 Defendants engaged in unfair, unlawful, or deceptive practices by failing to safeguard the PII of Plaintiffs and Class Members; and,

i. Whether Class Members are entitled to actual damages, statutory damages, injunctive relief, and/or punitive damages as a result of Defendants' wrongful conduct.

COUNT I
NEGLIGENCE
(On Behalf of Plaintiffs and the Nationwide Class)

98. Plaintiffs re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 97.

99. As a condition of their employment with Defendants, Defendants' current and former employees were obligated to provide Defendants with certain PII, including their names, Social Security numbers, driver's license numbers or government-issued identification numbers, financial account numbers provided for direct deposit, electronic signatures, and dates of birth, and those of their beneficiaries and dependents.

100. Plaintiffs and the Class Members entrusted their PII to Defendants on the premise and with the understanding that Defendants would safeguard their information, use their PII for business purposes only, and/or not disclose their PII to unauthorized third parties.

101. Defendants have full knowledge of the sensitivity of the PII and the types of harm that Plaintiffs and Class Members could and would suffer if the PII were wrongfully disclosed.

102. Defendants knew or reasonably should have known that the failure to exercise due care in the collecting, storing, and using of their current and former employees' PII, and that of their beneficiaries and dependents, involved an unreasonable risk of harm to Plaintiffs and Class Members, even if the harm occurred through the criminal acts of a third party.

103. Defendants had 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 Defendants' security protocols to ensure that Plaintiffs' and Class Members' information in Defendants' possession was adequately secured and protected.

104. Defendants also had a duty to exercise appropriate clearinghouse practices to remove former employees' PII, and that of their beneficiaries and dependents, they were no longer required to retain pursuant to regulations.

105. Defendants also had a duty to have procedures in place to detect and prevent the improper access and misuse of Plaintiffs' and Class Members' PII.

106. Defendants' duty to use reasonable security measures arose as a result of the special relationship that existed between Defendants and Plaintiffs and Class Members. That special relationship arose because Plaintiffs and Class Members entrusted Defendants with their confidential PII, a necessary part of employment with the company.

107. Defendants were subject to an "independent duty," untethered to any contract between Defendants and Plaintiffs or Class Members.

108. A breach of security, unauthorized access, and resulting injury to Plaintiffs and the Class Members was reasonably foreseeable, particularly in light of Defendants' inadequate security practices.

109. Plaintiffs and Class Members were the foreseeable and probable victims of any inadequate security practices and procedures. Defendants knew of should have known of the inherent risks in collecting and storing the PII of Plaintiffs and the Class, the critical importance of providing adequate security of that PII, and the necessity for encrypting PII stored on Defendants' systems.

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

111. Plaintiffs and the Class Members had no ability to protect their PII that was in, and possibly remains in, Defendants' possession.

112. Defendants were in a position to protect against the harm suffered by Plaintiffs and Class Members as a result of the Data Breach.

113. Defendants had and continue to have a duty to adequately disclose that the PII of Plaintiffs and Class Members within Defendants' 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 Members to take steps to prevent, mitigate, and

repair any identity theft and the fraudulent use of their PII by third parties.

114. Defendants had a duty to employ proper procedures to prevent the unauthorized dissemination of the PII of Plaintiffs and Class Members.

115. Defendants have admitted that the PII of Plaintiffs and Class Members was wrongfully lost and disclosed to unauthorized third persons as a result of the Data Breach.

116. Defendants, through their actions and/or omissions, unlawfully breached their duties to Plaintiffs and Class Members by failing to implement industry protocols and exercise reasonable care in protecting and safeguarding the PII of Plaintiffs and Class Members during the time the PII was within Defendants' possession or control.

117. Defendants improperly and inadequately safeguarded the PII of Plaintiffs and Class Members in deviation of standard industry rules, regulations, and practices at the time of the Data Breach.

118. Defendants failed to heed industry warnings and alerts to provide adequate safeguards to protect their current and former employees' PII, and that of their beneficiaries and dependents, in the face of increased risk of theft.

119. Defendants, through their actions and/or omissions, unlawfully breached their duty to Plaintiffs and Class Members by failing to have appropriate procedures in place to detect and prevent dissemination of their current and former employees' PII, and that of their beneficiaries and dependents.

120. Defendants breached their duty to exercise appropriate clearinghouse practices by failing to remove former employees' PII, and that of their beneficiaries and dependents, they were no longer required to retain pursuant to regulations.

121. Defendants, through their actions and/or omissions, unlawfully breached their duty

to adequately and timely disclose to Plaintiffs and Class Members the existence and scope of the Data Breach.

122. But for Defendants' wrongful and negligent breach of duties owed to Plaintiffs and Class Members, the PII of Plaintiffs and Class Members would not have been compromised.

123. There is a close causal connection between Defendants' failure to implement security measures to protect the PII of Plaintiffs and Class Members and the harm suffered or risk of imminent harm suffered by Plaintiffs and the Class. Plaintiffs' and Class Members' PII was lost and accessed as the proximate result of Defendants' failure to exercise reasonable care in safeguarding such PII by adopting, implementing, and maintaining appropriate security measures.

124. Additionally, 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 Defendants, of failing to use reasonable measures to protect PII. The FTC publications and orders described above also form part of the basis of Defendants' duty in this regard.

125. Defendants 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. Defendants' conduct was particularly unreasonable given the nature and amount of PII they obtained and stored and the foreseeable consequences of the immense damages that would result to Plaintiffs and Class Members.

126. Defendants' violation of Section 5 of the FTC Act constitutes negligence *per se*.

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

128. 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.

129. As a direct and proximate result of Defendants' negligence and negligence *per se*, 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 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 Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the current and former employees' PII, and that of their beneficiaries and dependents, in their continued possession; and (viii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PII compromised as a result of the Data Breach for the remainder of the lives of Plaintiffs and Class Members.

130. As a direct and proximate result of Defendants' negligence and negligence *per se*, Plaintiffs and Class Members 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.

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

COUNT II
BREACH OF CONTRACT
(On Behalf of Plaintiff Andre Samuel Hamid and the Contracted Employees Subclass)

132. Plaintiff Andre Samuel Hamid and the Contracted Employees Subclass re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 97.

133. Defendants entered into agreements with their current and former employees related to PII that these current and former employees provided to Defendants, including PII of the current and former employees and their beneficiaries and dependents.

134. Defendants and their current and former employees formed a contract when these current and former employees provided PII to Defendants subject to this agreement.

135. Defendants current and former employees fully performed their obligations under the contract with Defendants.

136. Defendants breached their agreement with their current and former employees by failing to protect their PII. Specifically, Defendants (1) failed to use reasonable measures to protect that information; and (2) disclosed that information to one or more unauthorized third parties, in violation of the agreement.

137. As a direct and proximate result of these breaches of contract, Defendants' current and former employees sustained actual losses and damages as described in detail above, including but not limited to that they did not get the benefit of the bargain.

COUNT III
BREACH OF CONTRACT
(On Behalf of Plaintiff Amy Lynn Hamid and the Third-Party Beneficiaries Subclass)

138. Plaintiff Amy Lynn Hamid and the Third-Party Beneficiaries Subclass re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 97.

139. Defendants entered into agreements with their current and former employees related to PII that these current and former employees provided to Defendants, including PII of the current and former employees and their beneficiaries and dependents.

140. Defendants and their current and former employees formed a contract when these current and former employees provided PII to Defendants subject to this agreement.

141. Defendants current and former employees fully performed their obligations under the contract with Defendants.

142. The contract was intended for the benefit of the beneficiaries and dependents of Defendants' current and former employees whose PII was provided to Defendants.

143. The benefit to the beneficiaries and dependents of Defendants' current and former employees was clear and direct, not incidental, indicating that Defendants assumed a duty to compensate these beneficiaries and dependents if the benefit was lost.

144. The beneficiaries and dependents of Defendants' current and former employees lost the benefit of the contract because Defendants failed to protect their PII. Specifically, Defendants (1) failed to use reasonable measures to protect that information; and (2) disclosed that information to one or more unauthorized third parties, in violation of the agreement.

145. As a direct and proximate result losing the benefit of the contract, the beneficiaries and dependents or Defendants' current and former employees sustained actual losses and damages as described in detail above, including but not limited to that they lost the benefit of the contract.

COUNT IV
Invasion of Privacy
(On Behalf of Plaintiffs and the Nationwide Class)

146. Plaintiffs re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 97.

147. Plaintiffs and Class Members had a legitimate expectation of privacy to their PII and were entitled to the protection of this information against disclosure to unauthorized third parties.

148. Defendants owed a duty to their current and former employees and their beneficiaries and dependents, including Plaintiffs and Class Members, to keep their PII contained as a part thereof, confidential.

149. Defendants failed to protect and released to unknown and unauthorized third parties the PII of Plaintiffs and Class Members.

150. Defendants allowed unauthorized and unknown third parties access to and examination of the PII of Plaintiffs and Class Members, by way of Defendants' failure to protect the PII.

151. The unauthorized release to, custody of, and examination by unauthorized third parties of the PII of Plaintiffs and Class Members is highly offensive to a reasonable person.

152. The intrusion was into a place or thing, which was private and is entitled to be private. Plaintiffs and Class Members disclosed their PII to Defendants as part of their employment with Defendant, but privately with an intention that the PII would be kept confidential and would be protected from unauthorized disclosure. Plaintiffs and Class Members were reasonable in their belief that such information would be kept private and would not be disclosed without their authorization.

153. The Data Breach at the hands of Defendants constitutes an intentional interference with Plaintiffs and Class Members' interest in solitude or seclusion, either as to their persons or as to their private affairs or concerns, of a kind that would be highly offensive to a reasonable person.

154. Defendants acted with a knowing state of mind when they permitted the Data Breach to occur because it was with actual knowledge that their information security practices were inadequate and insufficient.

155. Because Defendants acted with this knowing state of mind, they had notice and knew the inadequate and insufficient information security practices would cause injury and harm to Plaintiffs and Class Members.

156. As a proximate result of the above acts and omissions of Defendants, the PII of Plaintiffs and Class Members was disclosed to third parties without authorization, causing Plaintiffs and Class Members to suffer damages.

157. Unless and until enjoined, and restrained by order of this Court, Defendants' wrongful conduct will continue to cause great and irreparable injury to Plaintiffs and Class Members in that the PII maintained by Defendants can be viewed, distributed, and used by unauthorized persons for years to come. Plaintiffs and Class Members have no adequate remedy at law for the injuries in that a judgment for monetary damages will not end the invasion of privacy for Plaintiffs and the Class.

COUNT V
Breach of Confidence
(On Behalf of Plaintiffs and the Nationwide Class)

158. Plaintiffs re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 97.

159. At all times during Plaintiffs' and Class Members' interactions with Defendants, Defendants were fully aware of the confidential and sensitive nature of Plaintiffs' and Class Members' PII that Plaintiffs and Class Members employed by Defendants provided to Defendants.

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

161. Plaintiffs and Class Members employed by Defendants provided Plaintiffs' and Class Members' PII to Defendants with the explicit and implicit understandings that Defendants would protect and not permit the PII to be disseminated to any unauthorized third parties.

162. Plaintiffs and Class Members employed by Defendants also provided Plaintiffs' and Class Members' PII to Defendants with the explicit and implicit understandings that Defendants would take precautions to protect that PII from unauthorized disclosure.

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

164. Due to Defendants' failure to prevent and avoid the Data Breach from occurring, Plaintiffs' and Class Members' PII was disclosed and misappropriated to unauthorized third parties beyond Plaintiffs' and Class Members' confidence, and without their express permission.

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

166. But for Defendants' disclosure of Plaintiffs' and Class Members' PII in violation of the parties' understanding of confidence, their PII would not have been compromised, stolen,

viewed, accessed, and used by unauthorized third parties. Defendants' Data Breach was the direct and legal cause of the theft of Plaintiffs' and Class Members' PII as well as the resulting damages.

167. The injury and harm Plaintiffs and Class Members suffered was the reasonably foreseeable result of Defendants' unauthorized disclosure of Plaintiffs' and Class Members' PII. Defendants knew or should have known their methods of accepting and securing Plaintiffs' and Class Members' PII was inadequate as it relates to, at the very least, securing servers and other equipment containing Plaintiffs' and Class Members' PII.

168. As a direct and proximate result of Defendants' breach of their confidence with Plaintiffs and Class Members, 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 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 Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the PII of current and former employees and their beneficiaries and dependents; and (viii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PII compromised as a result of the Data Breach for the remainder of the lives of Plaintiffs and Class Members.

169. As a direct and proximate result of Defendants' breaches of confidence, Plaintiffs and Class Members 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.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, on behalf of themselves and all Class Members, request judgment against Defendants and that the Court grant the following:

A. For an Order certifying the Nationwide Class as defined herein, and appointing Plaintiffs and their Counsel to represent the Class;

B. For equitable relief enjoining Defendants from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiffs' and the Class Members' PII, and from refusing to issue prompt, complete, any accurate disclosures to Plaintiffs and the 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 Defendants from engaging in the wrongful and unlawful acts described herein;

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

iii. requiring Defendants to delete, destroy, and purge the personal identifying information of Plaintiffs and Class Members unless Defendants 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 Defendants to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of the personal identifying information of Plaintiffs and Class Members' personal identifying information;

v. prohibiting Defendants from maintaining Plaintiffs' and Class Members' personal identifying information on a cloud-based database;

vi. requiring Defendants 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 Defendants' systems on a periodic basis, and ordering Defendants to promptly correct any problems or issues detected by such third-party security auditors;

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

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

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

x. requiring Defendants to conduct regular database scanning and securing checks;

xi. requiring Defendants 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 personal identifying information, as well as protecting the personal identifying information of Plaintiffs and Class Members;

xii. requiring Defendants 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;

xiii. requiring Defendants to implement a system of tests to assess its respective employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees compliance with Defendants policies, programs, and systems for protecting personal identifying information;

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

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

xvi. requiring Defendants to implement logging and monitoring programs sufficient to track traffic to and from Defendants' 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 Defendants' 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; For an award of damages, including actual, nominal, and consequential damages, as allowed by law in an amount to be determined;

D. For an award of damages, including actual, nominal, and consequential damages, as allowed by law in an amount to be determined;

E. For an award of punitive damages;

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

G. For prejudgment interest on all amounts awarded; and

H. 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: December 31, 2020

Respectfully Submitted,

/s/ *Amanda Peterson*
AMANDA PETERSON (AP1797)
MORGAN & MORGAN
90 Broad Street, Suite 1011
New York, NY 10004
(212) 564-4568
apeterson@ForThePeople.com

JOHN A. YANCHUNIS
(*Pro Hac Vice application forthcoming*)
RYAN D. MAXEY
(*Pro Hac Vice application forthcoming*)

MORGAN & MORGAN
201 N. Franklin Street, 7th Floor
Tampa, Florida 33602
(813) 223-5505
jyanchunis@ForThePeople.com
rmaxey@ForThePeople.com

M. ANDERSON BERRY
(*Pro Hac Vice application forthcoming*)
CLAYEO C. ARNOLD,
A PROFESSIONAL LAW CORP.
865 Howe Avenue
Sacramento, CA 95825
(916) 777-7777
aberry@justice4you.com