UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF NEW YORK

AMY DALTON, on behalf of herself and all others similarly situated,	:	
	:	**Case No.:**
Plaintiff,	:	
v.	:	**CLASS ACTION COMPLAINT**
	:	
MORGAN STANLEY SMITH BARNEY, LLC,	:	**JURY TRIAL DEMANDED**
	:	
Defendant.	:	

Plaintiff Amy Dalton ("Plaintiff"), on behalf of herself and all others similarly situated, brings this class action lawsuit against Morgan Stanley Smith Barney, LLC ("Morgan Stanley" or "Defendant"), and alleges based upon personal information and belief and the investigation of counsel as follows:

INTRODUCTION

1. Amy Dalton, individually and on behalf of all others similarly situated, brings this class action on behalf of persons who have suffered, and continue to suffer, financial losses and increased data security risks that are a direct result of Defendant's egregious failure to safeguard its customers' highly sensitive personally identifiable information ("PII"), including but not limited to names, Social Security numbers, passport numbers, addresses, telephone numbers, email addresses, account numbers, dates of birth, income, asset values and holding information.

2. Morgan Stanley offers financial brokerage services throughout the United States. When individuals sign up for a Morgan Stanley account, they are required to provide Morgan Stanley PII for themselves and any other individuals associated with the account. Morgan Stanley

promises all customers that it will protect their PII by using "computer safeguards and secured files and buildings."

3. Notably, this case does not involve a breach of Morgan Stanley's computer system by a third party, but rather an unauthorized disclosure of the PII of Plaintiff and members of the proposed Class (as defined in Paragraph 56 below) to unknown third parties.

4. On or about July 10, 2020, Defendant began notifying various state Attorneys General and its customers about multiple data breaches that occurred as early as 2016. According to Defendant, the breaches related to PII maintained at two data centers Morgan Stanley had closed in 2016. Morgan Stanley advised Plaintiff and the Class that computer equipment it believed had been wiped clean of information "still contained some data," and further advised that the computer equipment in question was no longer in its possession.

5. The breaches were not limited to 2016. In 2019, Defendant disconnected and replaced multiple computer servers in various branch locations. According to Morgan Stanley's Chief Information Security Officer, Gerard Brady, the branch office servers Morgan Stanley disconnected in 2019 had a software flaw that left "previously deleted data" on the hard drives "in an unencrypted form." Defendant admits that some of those servers are missing (the 2016 and 2019 incidents will be collectively referred to as the "Data Breach").

6. By obtaining, collecting, using, and deriving a benefit from Plaintiff's and the Class' PII, Defendant assumed legal and equitable duties to those individuals. Defendant admits that the unencrypted PII that has "left [its] possession" included PII from the account holders and any "individual(s) associated with your account(s), including account names and numbers (at Morgan Stanley and any linked bank accounts), Social Security number, passport number, contact information, date of birth, asset value and holdings data." Despite the fact that the threat of a data

breach is a well-known risk, Morgan Stanley failed to take reasonable steps to adequately protect the ultra-sensitive, highly sought after PII of Plaintiff and the Class, who are now left to deal with the direct consequences of Defendant's Data Breach.

7. The missing equipment and servers contain everything unauthorized third parties need to illegally use Morgan Stanley's current and former customers' PII to steal their identities and to make fraudulent purchases, among other things.

8. Defendant's actions have left the PII of Plaintiff and the Class exposed and accessible to hackers. Consequently, Plaintiff and the Class have incurred, and will continue to incur, significant damages in taking protective measures to reduce the risk of identity theft and other fraudulent activity, among other things.

9. The Data Breach was the inevitable result of Defendant's lax approach to the security of Plaintiff's and the Class' PII, which was compromised due to Morgan Stanley's negligent and/or careless acts and omissions and the failure to protect customers' data.

10. In addition to Defendant's failure to prevent the Data Breach, Defendant failed to detect the Data Breach for years, and when it did discover the Data Breach, it took Defendant over a year to report it to the affected individuals and the states' Attorneys General.

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

12. Plaintiff seeks to recover the costs that she and others similarly situated have been forced to bear, and will be forced to bear, as a direct result of Defendant's Data Breach and to

obtain appropriate equitable relief to mitigate future harm that is certain to occur in light of the Data Breach.

13. Morgan Stanley disregarded the rights of Plaintiff and the Class by intentionally, willfully, recklessly, or negligently failing to take and implement adequate and reasonable measures to ensure that its customers' PII was safeguarded, failing to take available steps to prevent an unauthorized disclosure of data, and failing to follow applicable, required and appropriate protocols, policies and procedures regarding the encryption of data, even for internal use. As a result, the PII of Plaintiffs and Class Members was compromised through disclosure to an unknown third party. Plaintiff 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.

PARTIES

14. Plaintiff Amy Dalton is a citizen of Palm Beach Gardens, Florida. Plaintiff's account is no longer active, but Plaintiff received the Notice on or about July 10, 2020 advising that her PII was contained on the computers devices that were part of the Data Breach.

15. Defendant Morgan Stanley Smith Barney, LLC is a limited liability company organized under the laws of Delaware, with its principal place of business at 1585 Broadway, New York, NY 10036.

JURISDICTION AND VENUE

16. This Court has subject matter jurisdiction over this action pursuant to the Class Action Fairness Act, 28 U.S.C. § 1332(d). The aggregated claims of the individual Class Members exceeds the sum or value of $5,000,000 million, exclusive of interest and costs; there are more

than 100 putative Class Members; and minimal diversity exists because the majority of putative Class Members, including the Plaintiff, are citizens of a different state than Defendant.

17. This Court has personal jurisdiction over Defendant Morgan Stanley as it maintains its principal headquarters in New York, is registered to conduct business in New York, regularly conducts business in New York, and has sufficient minimum contacts in New York. Defendant intentionally avails itself of this jurisdiction by conducting Morgan Stanley's corporate operations here and promoting, selling, and marketing Morgan Stanley's services to residents of New York.

FACTUAL ALLEGATIONS

Background

18. Morgan Stanley is a multinational investment bank and financial services company with offices in over 40 countries and more than 60,000 employees. The firm's clients include corporations, governments, institutions, and individuals. Morgan Stanley ranked No. 62 in the 2019 Fortune 500 list of the largest United States corporations by total revenue.

19. Plaintiff and the Class Members, as current and former customers, relied on Defendant to safeguard their PII, only use it for legitimate business purposes, and to only make authorized disclosures of their PII.

20. Defendant had an obligation to use reasonable measures to ensure that Plaintiff's and Class Members' PII was not disclosed to third parties. Notably, Morgan Stanley's "Privacy Pledge" (https://www.morganstanley.com/privacy-pledge) highlights the secure nature of its information system:

> Morgan Stanley's long-standing commitment to safeguard the privacy of information our clients entrust to us is essential to our goal to be the world's first choice for financial services. Protecting the confidentiality and security of client information has always been an integral part of how we conduct our business worldwide.

> We pledge to continue to ensure that our global business practices protect your privacy.

21. Morgan Stanley's *U.S. Privacy Policy and Notice* ("Privacy Policy") which appears on its website, provides that Morgan Stanley "use[s] [customers'] personal information … to detect security incidents and protect against malicious, deceptive, fraudulent, or illegal activity." *See* (https://www.morganstanley.com/disclaimers/us-privacy-policy-and-notice.html). According to the Privacy Policy, Morgan Stanley claims it uses security measures that comply with federal law to protect customers' personal information:

> These measures include computer safeguards and secured files and buildings. We have policies governing the proper handling of customer information by personnel and requiring third parties that provide support to adhere to appropriate security standards with respect to such information.

22. Pursuant to its Privacy Policy, Morgan Stanley collects and maintains PII from its individual account holders, including but not limited to: "Social Security number and income;" "investment experience and risk tolerance;" and "checking account number and wire transfer instruction."

23. Individual account holders may also supply Morgan Stanley with personal identification (including passport numbers), mailing and billing addresses, telephone numbers, email addresses, birthdates, bank account numbers, and information related to specific assets and holdings.

The Data Breach

24. On or about July 10, 2020, Morgan Stanley sent customers a *Notice of Data Breach* ("Notice"). The Notice informed Plaintiff and the Class that:

> In 2016, Morgan Stanley closed two data centers and decommissioned the computer equipment that processed client information in both locations. As is customary, we contracted with

> a vendor to remove the data from the devices. We subsequently learned that certain devices believed to have been wiped of all information still contained some unencrypted data. We have worked with outside technical experts to understand the facts and any potential risks

25. On or about July 10, 2020, Defendant notified various state Attorneys General of another data breach incident. Specifically, in addition to the 2016 incident, Morgan Stanley's Chief Information Security Officer, Gerard Brady, reported that there had also been a data breach in 2019:

> Separately, in 2019, Morgan Stanley disconnected and replaced certain computer servers in local branch offices. Those servers had stored information on encrypted disks that may have included personal information. During a recent inventory, we were unable to locate a small number of those devices. The manufacturer subsequently informed us of a software flaw that could have resulted in small amounts of previously deleted data remaining on the disks in unencrypted form. We have worked with outside technical experts to understand the facts and any potential risks.

26. In the Notice it sent to customers (including Plaintiff) and the letters to state Attorneys General, Morgan Stanley admitted that the hardware involved in both the 2016 and 2019 incidents (i.e. the Data Breach) was no longer in its possession and "it is possible that data associated with your account(s), could have remained on some of the devices when they left our possession."

27. Morgan Stanley further admitted that the unencrypted PII on the hardware no longer in its possession included information from the account holder and any "individual(s) associated with your account(s), including account names and numbers (at Morgan Stanley and any linked bank accounts), Social Security number, passport number, contact information, date of birth, asset value and holdings data."

28. In response to the Data Breach, Morgan Stanley claims it has "instituted enhanced security procedures on your account(s), including continuous fraud monitoring and monitoring of information about malicious online activity and evidence of misuse of any Morgan Stanley data." Morgan Stanley also claims it has "taken steps to further strengthen controls aimed at reducing the risk that such an incident could occur in the future."

29. Notwithstanding Morgan Stanley's claims regarding steps it has taken since the Data Breach, the fact remains that the computer equipment containing Plaintiff's and the Class' unencrypted information is missing and that information may be used without Plaintiff's and the Class' authorization.

30. Notwithstanding Morgan Stanley's claims regarding steps it has taken since the Data Breach, the fact remains that Defendant did not use reasonable security procedures and practices necessary to protect and safeguard Plaintiff's and the Class' PII, which has left that PII subject to unauthorized use.

Prevention of Breaches

31. Defendant could have prevented the Data Breach if it had taken proper security measures. First, Defendant should have properly encrypted the information that was contained on the hardware and devices at issue. Second, Defendant should have properly secured the equipment that it decommissioned in 2016 and the equipment it disconnected and replaced in 2019. Third, Defendant should have made certain that all its data, including Plaintiff's and the Class' PII, contained on the hardware and devices at issue was destroyed.

32. Defendant's negligence in safeguarding its customers' PII is inexplicable in light of the numerous data breaches that have occurred in the past several years and the repeated warnings and alerts directed to companies and consumers regarding the need to take proper

measures to protect and secure data maintained electronically. Indeed, Morgan Stanley suffered such data breaches of customer PII two years prior to this Data Breach.

33. Defendant has acknowledged the sensitive and confidential nature of the PII at issue in the Data Breach, and the potential privacy and financial risks to its customers that may result from the misuse or inadvertent disclosure of such PII. Yet, Defendant failed to take the steps necessary to protect the Plaintiff's and the Class' PII from being compromised.

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

35. Defendant's failure to safeguard the Plaintiff's and the Class' PII will have long-term effects. 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

36. Consumers' PII is valuable to criminals, as reflected by the sale of such information on the dark web.

37. Social Security numbers are among the worst kind of personal information to have stolen because they may be used for a variety of fraudulent purposes and are difficult for an individual to change. The Social Security Administration has stated that the loss of an individual's Social Security number can lead to identity theft and financial fraud:

> Identity theft is one of the fastest growing crimes in America. 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.[1]

38. Further, it is difficult to change or cancel a stolen Social Security number. Obtaining a new Social Security number requires evidence of actual misuse. As a result, preventive action to defend against the possibility of misuse of a Social Security number is not permitted; rather, an individual must show evidence of fraudulent activity before being allowed to obtain a new number.

39. Even if an individual obtains a new Social Security number, there is no assurance that will prevent fraud relating to the old number because "credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[2]

40. The information compromised in the Data Breach is significantly more valuable to criminals than credit card information in a retailer data breach because unlike those situations where the victims can cancel or close credit and debit card accounts, the PII (Social Security number, passport number, name, date of birth, and various financial information) compromised here is impossible to close and extremely difficult to change. With the PII compromised here,

---

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

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

identity thieves can obtain driver's licenses, governmental benefits, medical services, and housing or even give false identification information to police.

41. The fraudulent activity resulting from the Data Breach may not be uncovered for years to come. Thus, there may be a time lag between when the harm occurs versus when it is discovered. There may also be a time lag between when PII is stolen and when it is used. According to the U.S. Government Accountability Office ("GAO"), which studied data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[3]

42. At all relevant times, Defendant knew, or reasonably should have known, of the importance of safeguarding its current and former customers' PII, including Social Security numbers and dates of birth, and of the foreseeable consequences that would occur if Defendant's data system was breached, including the substantial costs that would be imposed on Defendant's customers as a result of such a breach.

43. Plaintiff and the Class now face years of constant monitoring of their personal and financial records. Plaintiff and the Class are incurring and will continue to incur such damages in addition to any fraudulent use of their PII that may occur.

44. Defendant was, or should have been, fully aware of the unique type and the significant volume of data on Defendant's decommissioned equipment, amounting to potentially millions of individuals' personal and financial information.

---

[3] *Report to Congressional Requesters*, GAO, at 29 (June 2007) (http://www.gao.gov/new.items/d07737.pdf)

45. Defendant has offered customers affected by the Data Breach two years of credit monitoring service through a single credit bureau, Experian. This is not an adequate response to the potential harm that Plaintiffs and the Class will face for years to come because of their compromised PII.

46. The injuries to Plaintiff and the Class were directly and proximately caused by Defendant's failure to adequately safeguard its current and former customers' PII.

Plaintiff's Experience

47. In connection with the opening of her account at Morgan Stanley, Plaintiff provided Defendant with her PII, including her name, date of birth, and Social Security number.

48. Plaintiff received the Notice dated July 10, 2020 and reviewed the information Defendant provided her regarding the Data Breach.

49. Since the time that Plaintiff received the Notice, she has spent time related to the consequences of the Data Breach, including consulting with counsel about the potential harm that may arise as a result of the Data Breach and the possible actions needed to be taken to safeguard her as best as possible from identity fraud and financial fraud.

50. Plaintiff suffered actual injury and damages in paying money to Defendant in connection with her account before the Data Breach. Plaintiff would not have paid Defendant such money had Defendant disclosed that it lacked proper security protocol to safeguard customers' PII.

51. Plaintiff suffered actual injury in the form of damages to and diminution in the value of her PII, which was compromised because of the Data Breach.

52. Plaintiff suffered lost time, annoyance, and inconvenience because of the Data Breach, and has anxiety and concerns for the loss of her privacy.

53. Plaintiff has suffered imminent and impending injury resulting from the increased risk of fraud, identity theft, and misuse of her compromised PII.

54. Plaintiff 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.

CLASS ALLEGATIONS

55. Plaintiff brings this action on behalf of herself and as a class action under Federal Rules of Civil Procedure 23(a), (b)(2), and (b)(3), on behalf of the following nationwide class (the "Class"): "All individuals in the United States whose PII was compromised in the Data Breach disclosed by Morgan Stanley on or about July 10, 2020. Excluded from the Class are Defendant and Defendant's parents, subsidiaries, affiliates, officers and directors, current or former employees, and any entity in which Defendant has a controlling interest, and all federal, state or local governmental entities, 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."

56. This action may properly be maintained as a class action because it satisfies the requirements of Fed. R. Civ. P. 23(a): numerosity, commonality, typicality, and adequacy.

57. **Numerosity**. The members of the Class are so numerous and geographically dispersed throughout the United States that joinder of all members is impracticable.

58. **Commonality**. Questions of law and fact common to the Class exist, including, but are not limited to the following:

a. Whether Defendant owed a duty to Plaintiff and the Class to protect PII;

b. Whether Defendant failed to provide reasonable security to protect PII;

c. Whether Defendant negligently or otherwise improperly allowed third parties to access PII;

d. Whether Defendant failed to adequately notify Plaintiff and members of the Class that their data systems were breached;

e. Whether Plaintiff and members of the Class were injured and suffered damages and ascertainable losses;

f. Whether Defendant's actions, which failed to reasonably secure Plaintiff's and the Class's PII, proximately caused the injuries suffered by Plaintiff and members of the Class;

g. Whether Plaintiff and members of the Class are entitled to damages and, if so, the measure of such damages; and

h. Whether Plaintiff and members of the Class are entitled to declaratory and injunctive relief.

59. **Typicality**. Plaintiff's claims are typical of the claims of the absent class members and have a common origin and basis. Plaintiff and Class members are all persons and entities injured by Defendant's Data Breach. Plaintiff's claims arise from the same practices and course of conduct giving rise to the claims of the absent Class members and are based on the same legal theories, namely, Defendant's data breach. If prosecuted individually, the claims of each Class member would necessarily rely upon the same material facts and legal theories and seek the same relief.

60. **Adequacy**. Plaintiff will fully and adequately assert and protect the interests of the absent Class members and has retained Class counsel who have considerable experience in class action litigation concerning corporate data security and the resources necessary to prosecute this

case. Neither Plaintiff nor her attorneys have any interests contrary to or conflicting with the interests of absent class members.

61. This action may properly be maintained as a class action because the requirements of Fed. R. Civ. P. 23(b)(3) are satisfied.

62. **Predominance**. The questions of law and fact common to all Class members predominate over any questions affecting only individual class members.

63. **Superiority**. A class action is superior to all other available methods for the fair and efficient adjudication of this lawsuit because individual litigation of the absent Class members' claims is economically infeasible and procedurally impracticable. Class members share the same factual and legal issues and litigating the claims together will prevent varying, inconsistent, or contradictory judgments, and will prevent delay and expense to all parties and the court system through litigating multiple trials on the same legal and factual issues. Class treatment will also permit Class members to litigate their claims where it would otherwise be too expensive or inefficient to do so. Plaintiff knows of no difficulties in managing this action that would preclude its maintenance as a class action.

64. Contact information for each Class member, including mailing addresses, is readily available, facilitating notice of the pendency of this action.

COUNT I

NEGLIGENCE

65. Plaintiff incorporates by reference all the above allegations as if fully set forth herein.

66. As a condition of their using the services of Defendant, customers were obligated to provide Defendant with certain PII, including their date of birth, mailing addresses, Social Security numbers, passport numbers and personal financial information.

67. Plaintiff and the Class entrusted their PII to Defendant with the understanding that Defendant would safeguard their information, use their PII for business purposes only, and/or not disclose their PII to unauthorized third parties.

68. Defendant owed Plaintiff and the Class a common-law duty to exercise reasonable care in the collection and storage of their PII.

69. Defendant's duty included an obligation to take reasonable protective measures against the foreseeable risk to Plaintiff and the Class that harm would inevitably result if their PII was interfered with, stolen, or copied while in Defendant's possession.

70. Defendant 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 Defendant's security protocols to ensure that Plaintiff's and Class Members' information in Defendant's possession was adequately secured and protected.

71. Defendant's duty to act reasonably in collecting, storing, and protecting PII also arises under Section 5 of the FTC Act, 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.

72. Defendant also had a duty to have procedures in place to detect and prevent the improper access and misuse of Plaintiff's and the Class' PII.

73. Defendant knew or should have known that by collecting and storing PII, it created a valuable trove of information that was a foreseeable target for third-party interference, copying, or theft.

74. Defendant knew or reasonably should have known that the failure to exercise due care in the collecting, storing, and using of its customers' PII involved an unreasonable risk of harm to Plaintiff and the Class, even if the harm occurred through the criminal acts of a third party.

75. Defendant knew or should have known that companies possessing similar data troves have in fact been targeted for hacking in highly publicized data breaches, including Yahoo, Equifax, Wyndham, Home Depot, Sony, and Marriott, to name just a few. In fact, Defendant was involved in a data breach prior to the Data Breach at issue here.

76. Once Defendant chose to collect and store PII belonging to Plaintiff and the Class, only Defendant was able to secure this valuable data trove from the foreseeable risk of third-party interference, copying, or theft.

77. Plaintiff and the Class reasonably assumed that a major corporation like Morgan Stanley would adhere to basic industry standards with respect to the collection and storage of PII.

78. Defendant breached its common law and statutory duties by failing to use reasonable data collection, storage, and security practices.

79. A breach of security, unauthorized access, and resulting injury to Plaintiff and the Class was reasonably foreseeable, particularly because of Defendant's inadequate security practices and previous breach incidents involving Morgan Stanley customers' PII on stolen equipment.

80. As a direct and proximate result of Defendant's negligence, Plaintiff and the Class have been harmed in several ways. They are all now at an increased risk of being victims of identity theft, financial impersonation, and a variety of other fraudulent schemes, including those that use targeted phishing or social engineering techniques facilitated by the use of compromised PII elements against victims. To guard against the heightened risk of these crimes, Plaintiff and

the Class will need to invest more of their time and money on monitoring their finances, tax records, credit scores, and accounts of all types, including financial institutions, social media, loyalty programs, online retailers, and others.

81. Plaintiff and the Class have suffered, and continue to suffer, injury, including, but not limited to, investing time and money in cancelling payment cards, changing or closing accounts, and taking other steps to monitor their identities and protect themselves.

82. But for Defendant's negligence, the PII of Plaintiff and the Class would not have been exposed, or in the alternative, Plaintiff and the Class would have at least learned of the compromise at an earlier point in time when some of their damages may have been mitigated.

COUNT II

INVASION OF PRIVACY

83. Plaintiff incorporates by reference all the above allegations as if fully set forth herein.

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

85. Defendant owed a duty to its customers, including Plaintiff and the Class, to keep their PII contained as a part thereof, confidential.

86. Defendant failed to protect and released to unknown and unauthorized third parties the PII of Plaintiff and the Class.

87. Defendant allowed unauthorized and unknown third parties access to and examination of the PII of the Plaintiff and the Class because of Defendant's failure to protect the PII.

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

89. The intrusion was into a place or thing, which was private and is entitled to be private. Plaintiff and the Class disclosed their PII to Defendant as part of its use of Defendant's services, but privately with the intention that the PII would be kept confidential and would be protected from unauthorized disclosure. Plaintiff and the Class were reasonable in their belief that such information would be kept private and would not be disclosed without their authorization.

90. The Data Breach at the hands of Defendant constitutes an intentional interference with Plaintiff's and the Class' 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.

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

92. Because Defendant acted with this knowing state of mind, it had notice and knew that inadequate and insufficient information security practices would cause injury and harm to Plaintiff and the Class.

93. As a proximate result of the above acts and omissions of Defendant, the PII of Plaintiff and the Class was disclosed to third parties without authorization, causing Plaintiff and the Class to suffer damages.

94. Unless and until enjoined and restrained by order of this Court, Defendant's wrongful conduct will continue to cause great and irreparable injury to Plaintiff and the Class in that PII maintained by Defendant can be viewed, distributed, and used by unauthorized persons for years to come. Plaintiff 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 Plaintiff and the Class.

COUNT III

NEGLIGENCE *PER SE*

95. Plaintiff incorporates by reference all the above allegations as if fully set forth herein.

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

97. Defendant violated Section 5 of the FTC Act by failing to use reasonable measures to protect PII and not complying with applicable industry standards. Defendant's conduct was particularly unreasonable given the nature and amount of the PII it obtained and stored, and the foreseeable consequences of the Data Breach for companies of Defendant's magnitude, including, specifically, the damages that would result to Plaintiff and the Class due to the valuable nature of the PII at issue in this case.

98. Defendant's violations of Section 5 of the FTC Act constitute negligence *per se*.

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

100. The harm that occurred because 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, due to 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 Class.

101. As a direct and proximate result of Defendant's negligence *per se*, Plaintiff and the Class have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of choosing 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 remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to take appropriate and adequate measures to protect the PII of customers and former customers in its continued possession; (viii) future costs in terms of time, effort, and money that will be spent to prevent, detect, contest, and repair the impact of the PII compromised because of the Data Breach for the remainder of the lives of Plaintiff and the Class; and (ix) the diminished value of Defendant's goods and services they received.

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

COUNT IV

UNJUST ENRICHMENT

103. Plaintiff incorporates by reference all the above allegations as if fully set forth herein.

104. Plaintiff and the Class conferred a monetary benefit on Defendant. Specifically, they purchased goods and services from Defendant and provided Defendant with their PII. In exchange, Plaintiff and the Class should have received from Defendant the goods and services that were the subject of the transaction and should have been entitled to have Defendant protect their PII with adequate data security.

105. Defendant knew that Plaintiff and the Class conferred a benefit on Defendant and have accepted or retained that benefit. Defendant profited from the purchases and used the PII of Plaintiff and the Class for business purposes.

106. The amounts Plaintiff and the Class paid for Defendant's goods and services should have been used, in part, to pay for the administrative costs of data management and security, including the proper and safe disposal of Plaintiff's and the Class' PII.

107. Under the principles of equity and good conscience, Defendant should not be permitted to retain the money belonging to Plaintiff and the Class because Defendant failed to implement the data management security measures that are mandated by industry standards.

108. Defendant failed to secure the PII of Plaintiff and the Class and did not provide full compensation for the benefit Plaintiff and the Class provided to the Defendant.

109. Defendant acquired the PII through inequitable means because it failed to disclose the inadequate security practices previously alleged.

110. If Plaintiff and the Class knew that Defendant would not secure their PII using adequate security, they would not have made purchases or developed a financial relationship with Defendant.

111. Plaintiff and the Class have no adequate remedy at law.

112. As a direct and proximate result of Defendant's conduct, Plaintiff and the Class have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of choosing 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 remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to take appropriate and adequate measures to protect the PII of customers and former customers in its continued possession; (viii) future costs in terms of time, effort, and money that will be spent to prevent, detect, contest, and repair the impact of the PII compromised because of the Data Breach for the remainder of the lives of Plaintiff and the Class; and (ix) the diminished value of Defendant's goods and services they received.

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

114. Defendant should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiff and the Class, proceeds that it unjustly received from Plaintiff and the Class. Alternatively, Defendant should be compelled to refund the amounts that Plaintiff and the Class overpaid for Defendant's goods and services.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, individually and on behalf of the Class, respectfully requests that the Court:

A. Certify the Class and appoint Plaintiff and Plaintiff's counsel to represent the Class;

B. Enter a monetary judgment in favor of Plaintiff and the Class to compensate them for the injuries they have suffered, together with pre-judgment and post-judgment interest and treble damages and penalties where appropriate;

C. Enter a declaratory judgment as described herein;

D. Grant the injunctive relief requested herein;

E. Award Plaintiff and the Class reasonable attorneys' fees and costs of suit, as allowed by law; and

F. Award such other and further relief as this Court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiff demands a trial by jury on all claims so triable.

Date: August 14, 2020

Respectfully submitted,

/s/ Kyle A. Shamberg
Katrina Carroll*
Kyle A. Shamberg
CARLSON LYNCH LLP
111 W. Washington Street, Suite 1240
Chicago, Illinois 60602
Telephone: (312) 750-1265
Facsimile: (412) 231-0246
Email: kcarroll@carlsonlynch.com

Jonathan M. Jagher*
FREED KANNER LONDON

& MILLEN LLC
923 Fayette Street
Conshohocken, PA 19428
P. (610) 234-6487
jjagher@fklmlaw.com

William H. London*
Brian M. Hogan*
FREED KANNER LONDON
& MILLEN LLC
2201 Waukegan Rd, Suite 130
Bannockburn, IL 60015 USA
Phone: (224) 632-4500
Fax: (224) 632-4521
blondon@fklmlaw.com
bhogan@fklmlaw.com

Attorneys for Plaintiff and the Proposed Classes

*to be admitted *pro hac vice*