

James E. Cecchi  
**CARELLA, BYRNE, CECCHI,  
OLSTEIN, BRODY & AGNELLO, P.C.**  
5 Becker Farm Road  
Roseland, NJ 07068  
Telephone: (973) 994-1700  
Facsimile: (973) 994-1744  
Email: jcecchi@carellabyrne.com

**THE UNITED STATES DISTRICT COURT  
FOR THE SOUTHERN DISTRICT OF NEW YORK**

TIMOTHY M. SMITH on behalf of himself and all  
others similarly situated,  
  
Plaintiff,  
  
v.  
MORGAN STANLEY SMITH BARNEY, LLC,  
  
Defendant.

Case No.: \_\_\_\_\_

**CLASS ACTION COMPLAINT**

DEMAND FOR A JURY TRIAL

Plaintiff Timothy M. Smith (“Plaintiff”) brings this Class Action Complaint against Morgan Stanley Smith Barney, LLC (“Morgan Stanley”), as an individual and on behalf of all others similarly situated, and allege, on personal knowledge as to his own actions, the investigation of his attorneys, and upon information and belief as to all other matters, as follows:

**INTRODUCTION**

1. Plaintiff brings this class action against Morgan Stanley for its failure to properly secure and safeguard personal identifiable information, including names, Social Security numbers, passport numbers, addresses, telephone numbers, email addresses, account numbers, dates of birth, income, asset value and holding information (collectively, “personal identifiable information” or

“PII”). Plaintiff also alleges Defendant failed to provide timely, accurate, and adequate notice to Plaintiff and similarly situated Morgan Stanley current and former customers (“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. Morgan Stanley sells securities and other financial products throughout the world, maintaining offices nationwide and globally. When individuals register for a Morgan Stanley account, they are required to give the firm an extensive amount of PII for themselves and others associated with the account. Morgan Stanley retains this information on computer hardware—even after a customer closes an account— and promises the public it will protect “the confidentiality and security of client information” by, among other things, using “computer safeguards and secured files and buildings.”

3. This case does not involve a breach of a computer system by a third party, but rather an unauthorized disclosure of the PII of Plaintiff and the class by Defendant to unknown third parties.

4. On or about July 9, 2020, Morgan Stanley began notifying various state Attorneys General about multiple data breaches that occurred as early as 2016. Around the same time, Defendant mailed a *Notice of Data Breach* to current and former customers affected by the breaches. First, in 2016, Morgan Stanley closed two data centers and decommissioned the computer equipment. Morgan Stanley hired a vendor to remove customers’ data from the equipment. Subsequently, Morgan Stanley learned that the data was not fully “wiped” clean, and admits that “certain devices believed to have been wiped of all information still contained some unencrypted data.” Now, according to Defendant, that equipment is missing.

5. Second, in 2019, Morgan Stanley disconnected and replaced multiple computer servers in various branch locations. The old servers, which still contained customers' data, were thought to be encrypted, but Morgan Stanley subsequently learned that a "software flaw" on the servers left "previously deleted data" on the hard drives "in an unencrypted form." Now those servers are also missing (the 2016 and 2019 incidents will be collectively referred to herein as the "Data Breach").

6. By obtaining, collecting, using, and deriving a benefit from Plaintiff' and the Class Members' 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."

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. Not only can unauthorized third-parties access Defendant's customers' PII, the PII can be sold on the dark web. Hackers can access and then offer for sale the unencrypted, unredacted PII to criminals. Plaintiff and Morgan Stanley's current and former customers face a lifetime risk of identity theft, which is heightened here by the loss of customers' Social Security number.

9. This PII was compromised due to Morgan Stanley's negligent and/or careless acts and omissions and the failure to protect customers' data. In addition to Morgan Stanley's failure to prevent the Data Breach, Defendant failed to detect the Data Breach for years, and when they

did discover the Data Breach, it took them over a year, possibly longer, to report it to the affected individuals and the states' Attorneys General.

10. As a result of this delayed response, Plaintiff and Class Members were completely unaware 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 throughout their lives.

11. Plaintiff brings this action on behalf of all persons whose PII was compromised as a result of Defendant's failure to: (i) adequately protect its customers' PII; (ii) warn customers of its inadequate information security practices; and (iii) effectively secure hardware containing protected PII using reasonable and effective security procedures free of vulnerabilities and incidents. Defendant's conduct constitutes negligence, the proximate cause of which caused damages to Plaintiff and Class Members as alleged herein.

12. Alternatively, Defendant has been unjustly enriched. The amounts Plaintiff and Class Members 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 Class Members' PII. Under the principles of equity and good conscience, Defendant should not be permitted to retain the money belonging to Plaintiff and Class Members, because Defendant failed to implement the data management and security measures mandated by industry standards.

13. Plaintiff and Class Members have suffered injury as a result of Defendant's 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 on the missing equipment for unauthorized third parties to access and abuse; and (b) may remain backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII.

14. Morgan Stanley disregarded the rights of Plaintiff and Class Members 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 the result, the PII of Plaintiff and Class Members was compromised through disclosure to an unknown and unauthorized 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**

12. Plaintiff Timothy M. Smith is a citizen of the State of North Carolina, residing in Knightdale, North Carolina. Mr. Smith is the primary account holder of the Morgan Stanley IRA. This account is not still active. On or about July 15, 2020, Mr. Smith received Morgan Stanley's Notice of Data Breach, dated July 9, 2020. The notice specifically stated that his information associated with his account was likely subject to the Data Breach.

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

### **JURISDICTION AND VENUE**

14. This Court has subject matter 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 member of the class is a citizen of a state different from Defendant. Plaintiff is a citizen of North Carolina and therefore diverse from Defendant, which is headquartered in New York.

### **FACTUAL ALLEGATIONS**

15. Morgan Stanley is a multinational investment bank and financial services company with offices in over 40 countries with 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.

16. Plaintiff and the Class Members, as current and former customers, relied on this sophisticated Defendant 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. Customers demand security to safeguard their PII.

17. Defendant had a duty to adopt reasonable measures to protect Plaintiff's and Class Members' PII from involuntary disclosure to third parties. Morgan Stanley touts the secure nature of its system in its "Privacy Pledge":

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. (emphasis added)<sup>1</sup>

18. Morgan Stanley also claims that the firm “use[s] personal information . . . to detect security incidents and protect against malicious, deceptive, fraudulent, or illegal activity.”<sup>2</sup> The company further claims:

To protect your personal information from unauthorized access and use, we use security measures that comply with federal law. 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.<sup>3</sup>

19. 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 instructions.”<sup>4</sup>

20. Individual Morgan Stanley account holders may also supply the firm with personal identification (including passport numbers), mailing and billing addresses, telephone numbers, emails addresses, dates of birth, bank account numbers, and specific asset value and holdings information.

---

<sup>1</sup> Morgan Stanley's *Privacy Pledge*, available at: <https://www.morganstanley.com/privacy-pledge>

<sup>2</sup> Morgan Stanley's *U.S. Privacy Policy and Notice*, available at: <https://www.morganstanley.com/disclaimers/us-privacy-policy-and-notice.html>

<sup>3</sup> Morgan Stanley's *U.S. Customer Privacy Notice*, available at: <https://www.morganstanley.com/disclaimers/im-customer-privacy-notice.pdf>

<sup>4</sup> *Id.*

***The Data Breach***

21. Beginning on or about July 9, 2020, Morgan Stanley sent customers a *Notice of Data Breach*<sup>5</sup>. Morgan Stanley, identifying itself as “Morgan Stanley Smith Barney LLC. Member SIPC. / Morgan Stanley Private Bank, National Association. Member FDIC,” informed the recipients of the notice 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 [(the “Data Center Event”)].<sup>6</sup>

22. On or about July 10, 2020, Morgan Stanley sent data breach notifications to various state Attorneys General, including Iowa’s Attorney General Tom Miller, signed by Gerard Brady, Morgan Stanley’s Chief Information Security Officer. Brady reported the 2016 incident above and added information about another related breach that began in 2019:

Separately, in 2019, Morgan Stanley disconnected and replaced certain computer servers (the “WAAS device”) 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 (the “WAAS Device Event”).<sup>7</sup>

23. Morgan Stanley admitted in the Notice of Data Breach and the letters to the Attorneys General that the hardware involved in both the 2016 Data Center Event and the 2019

---

<sup>5</sup> See *Notice of Data Breach*, filed July 10, 2020 with the California Attorney General, a true and correct copy of which is attached hereto as Exhibit 1 (“Ex. 1”).

<sup>6</sup> Ex. 1, p. 1.

<sup>7</sup> See *Letter from Morgan Stanley’s Gerard Brady to Iowa’s Attorney General Tom Miller*, dated July 10, 2020, attached hereto as Exhibit 2 (“Ex. 2”).

WAAS Device Event “left our possession” at some point containing unencrypted information, and “it is possible that data associated with your account(s) could have remained on some of the devices when they left our possession.”<sup>8</sup>

24. Defendant further admitted that the unencrypted PII that left 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.”<sup>9</sup>

25. For an UTMA/CA account, for example, the lost PII would include PII belonging to the UTMA/CA custodian managing the account and the minor account holder.

26. 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.” It has also “taken steps to further strengthen controls aimed at reducing the risk that such an incident could occur in the future.”<sup>10</sup>

27. The equipment containing Plaintiff’s and Class Members’ unencrypted information is missing, and is or 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 affected customers’ approval. Unauthorized individuals can easily access Morgan Stanley’s customers’ unencrypted, unredacted information from these multiple devices, including Social Security numbers, passport numbers,

---

<sup>8</sup> Ex. 2

<sup>9</sup> Exs. 1, 2.

<sup>10</sup> Exs. 1, 2.

addresses, telephone numbers, email addresses, checking account numbers, dates of birth, income, asset value and holding information.

28. Defendant did not use reasonable security procedures and practices appropriate to the nature of the sensitive, unencrypted information it was maintaining for current and former customers, causing Plaintiff's and Class Members' PII to be exposed.

***Securing PII and Preventing Data Breaches***

29. Defendant could have prevented this Data Breach by properly encrypting the lost equipment and computer files containing PII on those lost hard drives. And, as Defendant claims it does, properly securing the "building" or location housing the equipment. Or Morgan Stanley could have destroyed the data.

30. Defendant's negligence in safeguarding its customers' PII is exacerbated by the repeated warnings and alerts directed to protecting and securing electronics. Indeed, Morgan Stanley suffered similar breaches just two years before the Data Breach that involved stolen equipment containing customer PII.<sup>11</sup>

31. Defendant has acknowledged the sensitive and confidential nature of the PII. To be sure, collection, maintaining, and protecting PII is vital to many of Defendant's business purposes. Defendant has acknowledged through conduct and statements that the misuse or inadvertent disclosure of PII can pose major privacy and financial risks to impacted individuals, and that under state law they may not disclose and must take reasonable steps to protect PII from improper release or disclosure. Despite the prevalence of public announcements of data breach and data security

---

<sup>11</sup> Aruna Viswanatha, *Morgan Stanley Fined \$1 Million for Client Data Breach*, The Wall Street Journal (2016), available at: <https://www.wsj.com/articles/morgan-stanley-fined-1-million-for-client-data-breach-1465415374>.

compromises, and despite its own acknowledgments of data security compromises, and despite their own acknowledgment of its duties to keep PII private and secure, Defendant failed to take appropriate steps to protect the PII of Plaintiff and the proposed Class from being compromised.

32. The Federal Trade Commission (“FTC”) defines identity theft as “a fraud committed or attempted using the identifying information of another person without authority.”<sup>12</sup> 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.”<sup>13</sup>

33. The ramifications of Defendant’s failure to keep its customers PII secure 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***

34. The PII of consumers 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.<sup>14</sup> Experian reports that a stolen credit or debit

---

<sup>12</sup> 17 C.F.R. § 248.201 (2013).

<sup>13</sup> *Id.*

<sup>14</sup> *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/>.

card number can sell for \$5 to \$110 on the dark web.<sup>15</sup> Criminals can also purchase access to entire company data breaches from \$900 to \$4,500.<sup>16</sup>

35. 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.<sup>17</sup>

36. Moreover, 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.

37. 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

---

<sup>15</sup> *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/>.

<sup>16</sup> *In the Dark*, VPNOverview, 2019, available at: <https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/>.

<sup>17</sup> Social Security Administration, *Identity Theft and Your Social Security Number*, available at: <http://www.ssa.gov/pubs/EN-05-10064.pdf>

new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number.”<sup>18</sup>

38. 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, passport number, name, date of birth, address, and asset holdings and other financial information.

39. 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.”<sup>19</sup>

40. 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.

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

---

<sup>18</sup> 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>.

<sup>19</sup> 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>

42. There may be a time lag between when harm occurs versus when it is discovered, and also between when PII is stolen and when it is used. According to the U.S. Government Accountability Office (“GAO”), which conducted a study regarding data breaches:

[L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.<sup>20</sup>

43. 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 security system was breached, including, specifically, the significant costs that would be imposed on Defendant’s customers as a result of a breach.

44. Plaintiff 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.

45. 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’ detailed, personal, finance-related information and thus, the significant number of individuals who would be harmed by the loss of decommissioned equipment containing unencrypted data.

46. To date, Defendant has offered its customers only two years of credit monitoring service through a single credit bureau, Experian. The offered service is inadequate to protect

---

<sup>20</sup> *Report to Congressional Requesters*, GAO, at 29 (June 2007), available at: <http://www.gao.gov/new.items/d07737.pdf>.

Plaintiff and Class Members from the threats they face for years to come, particularly in light of the PII at issue here.

47. The injuries to Plaintiff and Class Members were directly and proximately caused by Defendant's failure to implement or maintain adequate data security measures for its current and former customers' PII.

***Plaintiff Timothy Smith's Experience***

48. In or about September 23, 2004, Mr. Smith opened his Simple IRA retirement account at Morgan Stanley through his previous employer.

49. Mr. Smith supplied Morgan Stanley with his personal identifiable information, including but not limited to his address and Social Security number when he opened his account. The account no longer remains active as of the date of the filing of this Complaint.

50. Mr. Smith received the *Notice of Data Breach*, dated July 9, 2020. It was addressed to "Timothy Mark Smith Simple IRA dated 9/23/04."

51. As a result of the Data Breach notice, Mr. Smith spent time dealing with the consequences of the Data Breach, which includes time spent verifying the legitimacy of the *Notice of Data Breach* with counsel and time spent discussing the theft of his identity by a Georgia resident with North Carolina government officials, as set forth in the following paragraph. This time can never be recovered.

52. On or about July 13, 2020, and approximately two days prior to receiving the *Notice of Data Breach*, Mr. Smith was contacted by an official from the North Carolina Division of Employment Security (DES) who inquired about a discrepancy found in a filing for unemployment benefits with the Division linked to Mr. Smith's identity. After learning this information, Mr. Smith communicated to the DES official that he was in fact not requesting unemployment benefits,

and that the person in question residing in Georgia who was collecting those benefits was doing so under Mr. Smith's stolen identity.

53. Mr. Smith subsequently learned from North Carolina DES officials that the State of North Carolina had transmitted \$14,000 in unemployment benefits to a person in Georgia beginning in February 2000 who provided the Division with Mr. Smith's Social Security number, date of birth, and other relevant PII that is provided in order to obtain unemployment benefits in the State of North Carolina.

54. Mr. Smith is very careful about sharing his PII, and has never knowingly transmitted unencrypted PII over the internet or any other unsecured source.

55. Mr. Smith stores any and all information containing his PII in a safe and secure digital location, and destroys any documents he receives in the mail that contain any of his PII, or that may contain any information that could otherwise be used to compromise his credit card accounts and identity. Moreover, Mr. Smith diligently chooses unique usernames and passwords for his various online accounts.

56. Mr. Smith suffered actual injury and damages in paying annual fees to Defendant for facilitating his trading account before the Data Breach, expenditures that he would not have incurred had Defendant disclosed that it lacked data security practices adequate to safeguard customers' PII.

57. Mr. Smith suffered actual injury in the form of damages to and diminution in the value of his PII -- a form of intangible property -- that Mr. Smith entrusted to Morgan Stanley for the purpose of facilitating his trading account, which was compromised in the Data Breach.

58. Mr. Smith 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 and fact that

due to the Data Breach, a criminal stole his identity and is currently collecting unemployment benefits from the State of North Carolina under Mr. Smith's stolen identity.

59. Mr. Smith has suffered and will continue to suffer imminent and impending injury arising from the ongoing theft of his identity, which is compounded by the substantially increased risk of future fraud, identity theft, and misuse resulting from his PII, especially his Social Security number, being placed in the hands of criminals and other unauthorized third-parties.

60. Mr. Smith has a continuing interest in ensuring that his PII that remains backed up in Morgan Stanley's computer systems and is sufficiently protected and safeguarded from future data breaches.

### **CLASS ALLEGATIONS**

61. Plaintiff brings this nationwide class action on behalf of himself 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.

62. The Nationwide Class that Plaintiff seeks to represent is defined as follows:

All individuals whose PII was compromised in the data breach first announced by Morgan Stanley on or about July 9, 2020 (the "Nationwide Class").

63. Excluded from the Class are the following individuals and/or entities:

Defendant and Defendant's parents, subsidiaries, affiliates, officers and directors, current or former employees, and any entity in which Defendant has 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.

64. Plaintiff reserves the right to modify or amend the definition of the proposed classes before the Court determines whether certification is appropriate.

65. Numerosity, Fed R. Civ. P. 23(a)(1): The Nationwide Class is so numerous that joinder of all members is impracticable. Defendant has identified thousands of customers whose PII may have been improperly accessed in the Data Breach, and the Class is apparently identifiable within Defendant's records.

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

- a. Whether and to what extent Defendant had a duty to protect the PII of Plaintiff and Class Members;
- b. Whether Defendant had respective duties not to disclose the PII of Plaintiff and Class Members to unauthorized third parties;
- c. Whether Defendant had respective duties not to use the PII of Plaintiff and Class Members for non-business purposes;
- d. Whether Defendant failed to adequately safeguard the PII of Plaintiff and Class Members;
- e. Whether and when Defendant actually learned of the Data Breach;
- f. Whether Defendant adequately, promptly, and accurately informed Plaintiff and Class Members that their PII had been compromised;
- g. Whether Defendant violated their common law duties to Plaintiff and Class Members by failing to promptly notify Plaintiff and Class Members that their PII had been compromised;

- h. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;
- i. Whether Defendant adequately addressed and fixed the vulnerabilities which permitted the Data Breach to occur;
- j. Whether Plaintiff and Class Members are entitled to actual damages and/or punitive damages as a result of Defendant's wrongful conduct;
- k. Whether Plaintiff and Class Members are entitled to restitution as a result of Defendant's wrongful conduct;
- l. Whether Plaintiff and Class Members are entitled to injunctive relief to redress the imminent and currently ongoing harm faced as a result of the Data Breach.

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

68. Policies Generally Applicable to the Class: This class action is also appropriate for certification because Defendant has acted or refused to act on grounds generally applicable to the Class, thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward the Class Members, and making final injunctive relief appropriate with respect to the Class as a whole. Defendant's policies challenged herein apply to and affect Class Members uniformly and Plaintiff's challenge of these policies hinges on Defendant's conduct with respect to the Class as a whole, not on facts or law applicable only to Plaintiff.

69. Adequacy, Fed. R. Civ. P. 23(a)(4): Plaintiff 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. Plaintiff seeks 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. Plaintiff has retained counsel experienced in complex consumer class action litigation, and Plaintiff intends to prosecute this action vigorously.

70. 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 Defendant. Further, even for those Class Members who could afford to litigate such a claim, it would still be economically impractical and impose a burden on the courts.

71. The nature of this action and the nature of laws available to Plaintiff and Class Members make the use of the class action device a particularly efficient and appropriate procedure to afford relief to Plaintiff and Class Members for the wrongs alleged because Defendant would necessarily gain an unconscionable advantage since they would be able to exploit and overwhelm the limited resources of each individual Class Member with superior financial and legal resources; the costs of individual suits could unreasonably consume the amounts that would be recovered; proof of a common course of conduct to which Plaintiff was 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.

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

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

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

75. Further, Defendant has acted or refused to act on grounds generally applicable to the Class 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.

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

- a. Whether Defendant owed a legal duty to Plaintiff and Class Members to exercise due care in collecting, storing, using, and safeguarding their PII;

- b. Whether Defendant breached a legal duty to Plaintiff and Class Members to exercise due care in collecting, storing, using, and safeguarding their PII;
- c. Whether Defendant failed to comply with its own policies and applicable laws, regulations, and industry standards relating to data security;
- d. Whether an implied contract existed between Defendant on the one hand, and Plaintiff and Class Members on the other, and the terms of that implied contract;
- e. Whether Defendant breached their implied contract with Plaintiff and Class Members to adequately secure and protect Plaintiff' and Class Members' PII;
- f. Whether Defendant adequately, and accurately informed Plaintiff and Class Members that their PII had been compromised;
- g. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach; and
- h. Whether Class Members are entitled to actual damages, injunctive relief, and/or punitive damages as a result of Defendant's wrongful conduct.

**CLAIMS FOR RELIEF**

**COUNT I**

**Negligence**

**(On Behalf of Plaintiff and the Nationwide Class)**

77. Plaintiff re-alleges and incorporate by reference herein all of the allegations contained in the preceding paragraphs.

78. 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.

79. Plaintiff and the Class Members entrusted their PII to Defendant on the premise and 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.

80. Defendant has full knowledge of the sensitivity of the PII and the types of harm that Plaintiff and Class Members could and would suffer if the PII were wrongfully disclosed.

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

82. 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.

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

84. Defendant's duty of care arose as a result of, among other things, the special relationship that existed between Morgan Stanley and its clients. Defendant was in position to ensure that the PII of Plaintiff and Class Members was secure and that it was safeguarding and protecting such information from being compromised, lost, stolen, misused, and/or disclosed to unauthorized parties.

85. Defendant was subject to an "independent duty," untethered to any contract between Morgan Stanley and Plaintiff or Class Members.

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

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

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

89. Plaintiff and the Class Members had no ability to protect their PII that was in, and possibly remains in, Defendant's possession.

90. Defendant was in a position to protect against the harm suffered by Plaintiff and Class Members as a result of the Data Breach.

91. Defendant had and continues to have a duty to adequately disclose that the PII of Plaintiff and Class Members within Defendant's possession might have been compromised, how it was compromised, and precisely the types of data that were compromised and when. Such notice was necessary to allow Plaintiff 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.

92. Defendant had a duty to employ proper procedures to prevent the unauthorized dissemination of the PII of Plaintiff and Class Members.

93. Defendant has admitted that the PII of Plaintiff and Class Members was wrongfully lost and disclosed to unauthorized third persons as a result of the Data Breach.

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

95. Defendant improperly and inadequately safeguarded the PII of Plaintiff and Class Members in deviation of standard industry rules, regulations, and practices at the time of the Data Breach.

96. Defendant failed to heed industry warnings and alerts to provide adequate safeguards to protect customers' PII in the face of increased risk of theft.

97. Defendant, through its actions and/or omissions, unlawfully breached its duty to Plaintiff and Class Members by failing to have appropriate procedures in place to detect and prevent dissemination of its customers' PII.

98. Defendant, through its actions and/or omissions, unlawfully breached its duty to adequately and timely disclose to Plaintiff and Class Members the existence and scope of the Data Breach.

99. But for Defendant's wrongful and negligent breach of duties owed to Plaintiff and Class Members, the PII of Plaintiff and Class Members would not have been compromised.

100. There is a close causal connection between Defendant's failure to implement security measures to protect the PII of Plaintiff and Class Members and the harm suffered or risk

of imminent harm suffered by Plaintiff and the Class. Plaintiff and Class Members' PII was lost and accessed as the proximate result of Defendant's failure to exercise reasonable care in safeguarding such PII by adopting, implementing, and maintaining appropriate security measures.

101. As a direct and proximate result of Defendant's negligence, Plaintiff 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 Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII of customers in their continued possession; (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 Plaintiff and Class Members; and (ix) the diminished value of Defendant's goods and services they received.

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

**COUNT II**  
**Invasion of Privacy**  
**(On Behalf of Plaintiff and the Nationwide Class)**

103. Plaintiff re-alleges and incorporate by reference herein all of the allegations contained in the preceding paragraphs.

104. Plaintiff 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.

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

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

107. Defendant allowed unauthorized and unknown third parties access to and examination of the PII of Plaintiff and Class Members, by way of Defendant's failure to protect the PII.

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

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

110. The Data Breach at the hands of Defendant constitutes an intentional interference with Plaintiff 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.

111. 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.

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

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

114. 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 Class Members in that the 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**  
**(On Behalf of Plaintiff and the Nationwide Class)**

115. Plaintiff re-alleges and incorporate by reference herein all of the allegations contained in the preceding paragraphs.

116. 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.

117. 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 PII it obtained and stored, and the foreseeable consequences of the Data Breach for companies of Defendant’s magnitude, including, specifically, the immense damages that would result to Plaintiff and Class Members due to the valuable nature of the PII at issue in this case—including social security numbers.

118. Defendant’s violations of Section 5 of the FTC Act constitute negligence *per se*.

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

120. 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 its 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 Members.

121. As a direct and proximate result of Defendant’s negligence *per se*, Plaintiff 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 Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII of customers and former customers in its continued possession; (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 Plaintiff and Class Members; and (ix) the diminished value of Defendant's goods and services they received.

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

**COUNT IV**  
**Unjust Enrichment**  
**(On Behalf of Plaintiff and the Nationwide Class)**

123. Plaintiff re-alleges and incorporate by reference herein all of the allegations contained in the preceding paragraphs.

124. Plaintiff and Class Members conferred a monetary benefit on Defendant. Specifically, they purchased goods and services from Defendant and provided Defendant with their PII. In exchange, Plaintiff and Class Members 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.

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

126. The amounts Plaintiff and Class Members 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 and Class Members' PII.

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

128. Defendant failed to secure the PII of Plaintiff and Class Members and, therefore, did not provide full compensation for the benefit Plaintiff and Class Members provided.

129. Defendant acquired the PII through inequitable means in that it failed to disclose the inadequate security practices previously alleged.

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

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

132. As a direct and proximate result of Defendant's conduct, Plaintiff 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 Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII of customers and former customers in its continued possession; (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 Plaintiff and Class Members; and (ix) the diminished value of Defendant's goods and services they received.

133. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have suffered and will continue to suffer other forms of injury and/or harm, including,

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

### **PRAYER FOR RELIEF**

**WHEREFORE**, Plaintiff, on behalf of himself and all Class Members, request judgment against the Defendant and that the Court grant the following:

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

- a. For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiff's and

- the Class Members' PII, and from refusing to issue prompt, complete, any accurate disclosures to the Plaintiff and Class members;
- b. For equitable relief compelling Defendant to use appropriate cyber security methods and policies with respect to PII collection, storage, protection, and disposal, and to disclose with specificity to Plaintiff and Class Members the type of PII compromised;
  - c. 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 punitive damages;
  - e. For an award of attorneys' fees, costs, and litigation expenses, as allowed by law;
  - f. For prejudgment interest on all amounts awarded; and
  - g. Such other and further relief as this Court may deem just and proper.

**DEMAND FOR JURY TRIAL**

Plaintiff hereby demands that this matter be tried before a jury.

Date: August 27, 2020

Respectfully Submitted,

/s/ James E. Cecchi

James E. Cecchi

5 Becker Farm Road

Roseland, New Jersey 07068

Telephone: (973) 994-1700

Facsimile: (973) 994-1744

Email: jcecchi@carellabyrne.com

*Counsel for Plaintiff and the Proposed Class*