UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF NEW YORK

In re Morgan Stanley Data Security Litigation	20 Civ. 5914 (AT)

CONSOLIDATED AMENDED CLASS ACTION COMPLAINT

TABLE OF CONTENTS

Plaintiffs John and Midori Nelson, Sylvia Tillman, Mark Blythe, Vivian Yates, Cheryl and Richard Gamen, Amresh Jaijee, Richard Mausner, Desiree Shapouri, and Howard Katz (collectively, "Plaintiffs") bring this Consolidated Amended Class Action Complaint against Morgan Stanley Smith Barney, LLC ("Morgan Stanley" or "Defendant"), as individuals and on behalf of all others similarly situated. In addition to the named Plaintiffs, other recipients of Morgan Stanley's July 2020 letter disclosing the violations alleged herein (the "Notice Letter"), who are all members of the proposed class, have contacted Plaintiffs' counsel and Morgan Stanley with respect to the harm to them that resulted from those violations, including identity fraud. Some of their statements are referenced in paragraphs 23-24 below. Plaintiffs allege, upon personal knowledge as to their own actions and their counsel's investigations, and upon information and belief as to all other matters, as follows:

INTRODUCTION

1. In 2016, Morgan Stanley generated a net income of $6,000,000,000. That same year, in an attempt to save approximately $100,000 in the decommissioning of two of its data centers (the "Decommissioning"), Morgan Stanley made a series of reckless business decisions that ultimately resulted in the compromise of the confidential personally identifiable and financial information ("PII") of over 14 million of its current and former clients ("The 2016 Data Security Incident").

2. Rather than follow accepted industry standards or its internal protocols, Morgan Stanley: (i) terminated a contract with IBM for the decommissioning, wiping, and destruction of computer equipment storing PII; (ii) hired a local moving company with no information technology asset disposal ("ITAD") experience to handle the project; and (iii) failed to supervise the project. Morgan Stanley feigned shock when it learned two years later from a third party who

had purchased the used Morgan Stanley equipment that he had access to sensitive Morgan Stanley data.

3. To this day, as a result of Morgan Stanley's systemic failures and lack of inventory records, thousands of pieces of IT equipment containing unencrypted Morgan Stanley client PII remain completely unaccounted for. Many of these devices have been offered for sale on the internet and remain in the hands of third-party purchasers who now have unfettered access to the PII of millions of Morgan Stanley's former and current clients.

4. Morgan Stanley publicly acknowledges its fiduciary relationship with clients for whom it acts as an investment adviser.[1] Those clients, including the named Plaintiffs and Class Members, some of whom are referenced below, had good reason to believe that Morgan Stanley complied with financial industry standards governing the security of client data. In its "Privacy Pledge" to its clients as of March 17, 2016, Morgan Stanley promised:

> 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.[2]

5. In its U.S. Customer Privacy Notice, which federal law requires Morgan Stanley to disseminate, the company further claims:

---

[1] *See Morgan Stanley Important Account Information*, at 16 (*available at* https://www.morganstanley.com/wealth/relationshipwithms/pdfs/important_account_information.pdf) (last visited June 10, 2021).

[2] Morgan Stanley's *Privacy Pledge* as of March 17, 2016, *available at*: https://web.archive.org/web/20160317092855/https://www.morganstanley.com/privacy-pledge (emphasis added) (last visited June 14, 2021).

> 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.[3]

Yet, when questioned by the New York Attorney General about the 2016 Data Security Incident, Morgan Stanley disclosed that it had relied on outdated equipment that did not support encryption, and that encryption would have reduced the equipment's processing speed.

6. As data security became a heightened concern for all financial institutions, and others were expanding their efforts to safeguard their clients' PII, Morgan Stanley in 2016 slashed its information technology security budget by 30 percent. Incredibly, Morgan Stanley chose to make decommissioning assets a "profit center" for the company, rather than abide by industry standards for the destruction and disposal of used equipment.

7. The sequence of events that directly precipitated and followed the 2016 Data Security Incident reflects a pervasive culture of dereliction among the Morgan Stanley personnel charged with protecting its clients' PII:

a. In September 2015, less than a year before the 2016 Data Security Incident, an internal report deemed Morgan Stanley "non-compliant" with respect to industry standards and internal policies guiding the decommissioning and disposal of computer assets containing client data.

b. Morgan Stanley's failures were exacerbated by its failure to encrypt much of that data on the servers involved in the 2016 Data Security Incident.

[3] Morgan Stanley's *U.S. Customer Privacy Notice, available at* https://www.morganstanley.com/disclaimers/im-customer-privacy-notice.pdf (last visited May 13, 2021).

c. Despite IBM's management of the data centers, prior involvement in decommissioning devices, and submission of a bid to decommission and dispose of the Morgan Stanley equipment for the final stage of the Decommissioning, Morgan Stanley selected Triple Crown, a local mover with no relevant expertise, noting that using Triple Crown would result in a "saving[s] of $116,867."

d. Instead of complying with industry standards, which advise the physical destruction of used data storage equipment as the most secure means for its disposal, Morgan Stanley allowed for the devices to be wiped and resold, but failed to confirm the wiping was actually performed or alternatively that the equipment was destroyed.

e. Despite additional industry standards recommending that data be wiped or removed from equipment on-site before sending it offsite for disposal, Morgan Stanley delegated but failed to supervise that effort, and relinquished possession of its equipment to Triple Crown with its clients' PII remaining unencrypted on the devices.

f. Throughout the course of the Decommissioning, Morgan Stanley knew that Triple Crown was using WeedHire (formerly known as AnythingIT), whose primary business involved the cannabis industry, to assist in the disposal and resale of Morgan Stanley's used devices. Although Morgan Stanley had previously deemed WeedHire/AnythingIT a "high risk" and unsuitable vendor, Morgan Stanley raised no objection to its work on the project. In fact, Morgan Stanley continued directly contracting with WeedHire by selling its used equipment to WeedHire through Morgan Stanley's online auctions.

g. As a result of Morgan Stanley's disregard for industry standards, equipment containing unencrypted client PII was offered for sale on the internet, and was in fact sold to scores of purchasers, some in foreign countries known to be cybercrime havens.

h. Morgan Stanley learned that its clients' PII was in the hands of an unauthorized third party in October 2017, when "Mr. Oklahoma," who worked for an Oklahoma company that purchased some of Morgan Stanley's used equipment online from a reseller, emailed:

> I am sending this as a courtesy to you. I recently purchased NetApp gear from eBay. *[Upon turning it on], I had access to all of your data that was on the [equipment]* sold to us from a third party. I assume you sold the equipment to someone that sold you their services to destroy data. If so, I can assure you they breached said contract. If on the other hand, you sold them without something in place, you should have at least zeroed out the disks. I do not intend to make this public, nor should it, but you are a major financial institution and should be following some very stringent guidelines on how to deal with retiring hardware. Or at the very least getting some type of verisifaction [sic] of data destruction from the vendors you sell equipment to. I look forward to hearing from you.

Morgan Stanley personnel initially treated it as a "ransom email," and Morgan Stanley's then-Managing Director of Technology and Information Risk (the "Director") wrote: "I still don't believe in good Samaritans."

i. The Director emailed Mr. Oklahoma and requested pictures of labels and serial numbers to prove that the equipment he had purchased on eBay was Morgan Stanley decommissioned equipment. Mr. Oklahoma immediately complied, sending the Director unequivocal evidence that he had possession of Morgan Stanley's used computer equipment containing Morgan Stanley data.

j. Morgan Stanley did not ask Mr. Oklahoma to stop using the equipment. It did not arrange to promptly inspect or retrieve the equipment. It did not contact Mr. Oklahoma's employer, the legal purchaser and owner of the equipment. Instead, knowing that Mr. Oklahoma and others had unfettered access to client PII, Morgan Stanley had no further contact with Mr. Oklahoma for six weeks.

k. When Morgan Stanley finally decided to retrieve the equipment, it did so only after having Mr. Oklahoma destroy any physical evidence that Morgan Stanley client data had existed on the drives in his possession before they were returned. Morgan Stanley paid Mr. Oklahoma approximately $40,000 for these efforts.

l. Mr. Oklahoma stated under oath that he had been using the drives and did not return them immediately because the Morgan Stanley Director told him to do so: "After I sent the pictures and everything, he said, go ahead and use them . . . so I was using them. Then in about December he stated that they needed all the drives back."

m. Morgan Stanley finally retrieved the equipment in January 2018, three months after Mr. Oklahoma's initial email, and only after it had given time for Morgan Stanley's client data to be erased and rewritten, and evidence spoliated.

n. Despite these efforts, when returned to Morgan Stanley, some of the devices still contained its clients' PII, but Morgan Stanley worked with a supposedly independent forensic firm to exonerate Morgan Stanley as the source of that PII because the dataset included information Morgan Stanley claimed it would not normally store for clients.

o. Countless other internet purchasers still have Morgan Stanley's decommissioned assets. The whereabouts of this equipment—over 2,000 individual IT Assets—remains unknown.

p. Plaintiffs' counsel, through their investigation, recently recovered some of the missing devices from a third-party internet purchaser. The expert analysis of these devices is unequivocal: the PII (including Social Security numbers) is unencrypted and accessible. In fact, the data residing on these devices includes unencrypted PII, including Social Security numbers, banking information, addresses and telephone numbers, and account numbers, for hundreds of thousands of individuals. Indeed, while the review is not yet complete, this type of unencrypted PII for one of the named Plaintiffs in this case has been found on those drives, alongside the name of his Morgan Stanley broker.

8. Although Morgan Stanley filed a claim with its insurance carrier relating to the 2016 Data Security Incident in 2018—shortly after Mr. Oklahoma contacted it about the used, unwiped, and unencrypted equipment he had purchased—Morgan Stanley did not provide notice to its clients until more than four years after the Incident occurred and only as a result of being compelled to do so.[4]

9. Specifically, rather than comply with its statutory duty to promptly report the 2016 Data Security Incident and to notify millions of current and former clients to whom it owed a fiduciary duty, Morgan Stanley chose not to disclose the Incident until the summer of 2020, when the Office of the Comptroller of Currency ("OCC") compelled Morgan Stanley to do so.

[4] *See* OCC Consent Order (Oct. 8, 2020) ("Consent Order"), *available at* https://www.occ.gov/static/enforcement-actions/ea2020-058.pdf (last visited June 30, 2021).

10. The lessons to be learned from the 2016 Data Security Incident, like prior Morgan Stanley data security incidents,[5] were lost on Morgan Stanley. Three years later, in 2019, Morgan Stanley again failed to safeguard its clients' PII by failing to maintain proper documentation and inventory of assets during a decommissioning and disposal project and again losing track of thousands of those assets (hereafter the "the 2019 Data Security Incident").[6]

11. The vast majority of the missing computer equipment from both Incidents, which amounts to thousands of devices, remains unaccounted for.

12. To this day, not all of the Morgan Stanley clients who were victims of the 2019 Data Security Incident have been notified.

13. Numerous Morgan Stanley clients who were notified of the Data Security Incidents contacted Morgan Stanley to report various forms of identity theft that they attributed to those Incidents.[7] Those incidents spanned the entire period following the 2016 Data Security Incidents, and included such violations as: the submission of fraudulent tax returns using clients' Social Security numbers; the establishment of fraudulent financial accounts; fraudulent applications for employment benefits; and the successful submission of fraudulent loan applications.

[5] *See infra* ¶¶ 244-248.

[6] Due to its lack of proper record keeping, it was not until weeks after Morgan Stanley began notifying its clients about the Data Security Incidents, that it was able to ascertain from outside auditors that these additional computer servers contained client PII. Weeks later, certain Plaintiffs filed the first lawsuits against Morgan Stanley concerning both Data Security Incidents. As a direct result of Plaintiffs' ongoing investigation of the facts of this case, as documented herein, Morgan Stanley is currently in the process of identifying and notifying additional victims of the 2019 Data Security Incident.

[7] *See infra* ¶ 23.

14. The Data Security Incidents were not the first, or last, serious data security incidents experienced by Morgan Stanley. The company experienced numerous other privacy incidents during the same time period, reflecting its ongoing disregard for the safeguarding of client PII.

15. On October 8, 2020, Morgan Stanley entered into a Consent Order with the OCC concerning the Data Security Incidents. The OCC was clear in its findings:

> In connection with the [2016] decommissioning, [Morgan Stanley], among other things, failed to effectively assess or address the risks associated with the decommissioning of its hardware; failed to adequately assess the risk of using third party vendors, including subcontractors; and failed to maintain an appropriate inventory of customer data stored on the devices.[8]

16. The OCC further found that Morgan Stanley "failed to exercise adequate due diligence in selecting the third-party vendor engaged by Morgan Stanley and failed to adequately monitor the vendor's performance."[9]

17. The OCC, in assessing a civil penalty of $60 million against Morgan Stanley, noted that Morgan Stanley repeated those same mistakes in 2019: "In 2019, [Morgan Stanley] experienced similar vendor management control deficiencies in connection with the decommissioning of wide area application services devices."[10]

18. The OCC further found that Morgan Stanley did not inform potentially impacted customers of the 2016 Data Security Incident until it was compelled to do so "at the OCC's direction."[11] Thus, despite having reliable information as far back as October 2017, when it learned from Mr. Oklahoma that its clients' PII was in the possession of unauthorized third

---

[8] Consent Order, at 2.

[9] *Id.*

[10] *Id.*

[11] *Id.*

parties, and despite having filed a claim with its insurance carrier in 2018, Morgan Stanley failed to inform its clients—whose PII was divulged by the Incident, to whom it owed a fiduciary duty, and whose privacy it had pledged to safeguard—until it was compelled to do so by the OCC.

19. Morgan Stanley had a clear fiduciary duty to adopt, implement, and maintain reasonable measures to protect its clients' PII from unlawful disclosure to third parties. Morgan Stanley breached its fiduciary duties, resulting in a perpetual risk to its clients, Plaintiffs, and Class Members that their Social Security numbers, passport numbers, bank account numbers, contact information, dates of birth, asset value and holdings data and other PII that Morgan Stanley failed to encrypt and allowed to be divulged to unauthorized third parties is now forever at risk of misuse.

20. Had they been aware that Morgan Stanley's representations as to its data security were deceptive or materially misleading, Plaintiffs and Class Members would have taken their business elsewhere, or at a minimum paid Morgan Stanley less than they did for its services.

21. The OCC levied a civil penalty of $60,000,000 on Morgan Stanley for its conduct related to the two Data Security Incidents, which was at the time an unprecedented amount in the history of the agency.[12]

22. Morgan Stanley has acknowledged to the Arkansas Attorney General that "during its investigation, Morgan Stanley discovered that fragments of previously deleted, unencrypted data was possibly resident on the devices." Such "fragments" are thousands, if not millions, of 4,000-character blocks of PII.

[12] *Id.*

23. Morgan Stanley internal documents reflect that dozens of its clients put Morgan Stanley on notice that the Data Security Incidents resulted in their being victimized by identity fraud. By way of example only, those communications include the following:

- [MK] reported that his "social security number has been stolen and someone has filed for unemployment under his name," as a result of the 2016 Data Security Incident.
- [DRL] reported that "his daughter's SSN had been compromised because her taxes were rejected this year with the note that her SSN was already being used."
- [CC] reported that she "received a communication from IRS regarding a fraudulent account set up for an account she set up with the IRS," which she attributed to the Data Security Incidents.
- [DP] "complained to [the Consumer Financial Protection Bureau]" about the 2016 Data Security Incident and "[sent] his identity theft filings to [the FTC]."
- [CR] said that the Data Security Incidents had "caused multiple instances of her information being compromised."
- [EK] reported that she was a victim of identity theft due to the Data Security Incidents, as someone "opened a PayPal merchant account using her name, SSN, address, and phone number."
- [LE] said that her Social Security number was compromised as a result of the Data Security Incidents.
- [CF] said that, as a result of the Data Security Incidents, "her identity has been stolen and that someone has attempted to try and open 4 lines of credit in her name."

24. Several Class Members have contacted Plaintiffs' counsel. One reported that, shortly after Morgan Stanley disclosed the Data Security Incidents, she was notified that her

Social Security number had been used to apply for a $20,000 SBA loan. Another class member, an attorney whose father had established a Morgan Stanley account for her when she was a minor, had her Social Security number used in failed attempts to open credit card and other accounts. Another victim learned from a collection agency that thieves had secured a loan in his name and had opened a bank account in his name, using his Social Security number.

25. Plaintiffs and Class Members, which consist of current and former Morgan Stanley clients, have suffered concrete harm as a result of the Data Security Incidents.

A. The 2016 Data Security Incident

26. The 2016 Data Security Incident reflects systemic shortcomings in Morgan Stanley's asset disposal and data security practices. PricewaterhouseCoopers ("PwC") determined that Morgan Stanley "fail[ed] to ensure that devices containing data were wiped or physically destroyed prior to Morgan Stanley surrendering control over them" and that "[t]here was no clear ownership of the [vendor] contractual relationship."

27. An internal 2015 Technology and Information Risk department report references a general "[l]ack of evidence to demonstrate compliance with procedure requirements to wipe/degauss assets prior to disposal/reuse," and adds that "[r]esponsibility/accountability for key activities related to Data Decommissioning require [sic] additional clarity in Firmwide procedures."

28. An executive director of that department subsequently observed that:

- "we fail badly in server (70% failure rate)" and "[s]torage is not encrypted;"
- "[Enterprise Infrastructure] exhibited some confusion over who does what;"
- "[Enterprise Infrastructure] says they have no inventory of every device in the data center."

29. A year later, Morgan Stanley had done nothing to mitigate this problem. Instead, "EI [Enterprise Infrastructure] wanted risk to accept PCCT's [Policy Compliance Control Testing] data deco findings as low. They do not agree with PCCT's findings of 70% failure rate . . . [instead] this is a record keeping problem, and they cannot track storage component[s] in sufficient detail to through [sic] the entire lifecycle." Morgan Stanley's failure to track its inventory led directly to the 2016 Data Security Incident. "Servers that are off-net are out of sight and out of mind."

30. The lack of encryption proved devastating. Morgan Stanley told the New York Attorney General that "the generation of the hardware in use at the time did not support encryption" and that "other encryption technology would have significantly slowed the devices' processing." It also told the New Jersey Attorney General that encryption would have "prohibitively impacted performance." Clearly, Morgan Stanley favored efficiency and reduced costs over its clients' data security.

31. Prior to the Data Security Incidents, Morgan Stanley undertook a project to close several of its IBM-managed data centers and decommission or move its IT Assets housed at those centers.

32. The Decommissioning was scheduled to accelerate on March 23, 2016. Rather than maintain its relationship with IBM, Morgan Stanley solicited bids for the project. On March 22, 2016, Morgan Stanley rejected IBM's bid to continue its work in the Decommissioning. The Morgan Stanley Vice President charged with overseeing the Decommissioning (the "VP") determined that by using Triple Crown, a local moving company, instead of IBM, Morgan Stanley would save approximately $100,000. At the VP's direction, Triple Crown began taking

Morgan Stanley's equipment from the IBM facilities in Poughkeepsie, New York and Columbus, Ohio the following day.[13]

33. On April 8, 2016, the VP reported the estimated cost of the Decommissioning and was told, "[t]hat number is insane. We could just leave it laying there and not distroy [sic] it and pay for hotel cheaper than that. . . ." the VP responded, "btw, we can always hammer the vendors . . . ." The response the VP received was that an Enterprise Infrastructure executive "flipped at the cost of just killing these, so I expect he is going to com[e] knocking to see how we can get this cheaper." The VP responded, "ok, go[od] to know. I'll start squeezing now then."

34. Over the next six months, Morgan Stanley and Triple Crown would embark on a mass decommissioning of the remaining 4,900 IT Assets in these data centers.

35. The contract with Triple Crown provided that Triple Crown would resell the decommissioned equipment, with Morgan Stanley receiving 75% of the resulting revenue. This again is contrary to ITAD standards, which recommend destruction of decommissioned assets containing PII.

36. Triple Crown used WeedHire/AnythingIT as an ITAD partner at Morgan Stanley's request. Multiple documents submitted to Morgan Stanley during this process plainly show that Triple Crown used WeedHire/Anything IT for the retrieval and disposal of the IT Assets, which put Morgan Stanley on written notice that WeedHire/AnythingIT was the recipient of Morgan Stanley's unwiped, unencrypted IT Assets.

37. Morgan Stanley failed to object to the use of WeedHire/AnythingIT, despite the fact that Morgan Stanley had undertaken a risk assessment of AnythingIT in October 2014 and

[13] The VP has since been fired. Morgan Stanley's investigation of the Incident determined that the VP "failed to supervise Triple Crown's compliance with its contractual obligations…in several respects."

found it be a "high risk" vendor, noting that AnythingIT "[did] not seem to be focused on the data destruction business[, having changed] their priorities to . . . [being a] legalized marijuana job bank." The Morgan Stanley risk assessment further opined, "[t]he optics of using a company like this, that will handle Firm or client data, does not seem right for it could present franchise risk to Morgan Stanley." The final recommendation was that Morgan Stanley should "not do[] business with AnythingIT" going forward. Yet, Morgan Stanley employees continued contracting with WeedHire/AnythingIT, and Morgan Stanley continued selling used equipment to the company.

38. After Mr. Oklahoma contacted Morgan Stanley regarding his possession of equipment containing client PII, the VP—who had been in charge of the Decommissioning and vendor selection for the project— asked others at Morgan Stanley whether the drives had been wiped prior to being sent to Triple Crown. The VP was told that the drives had not been wiped and that Morgan Stanley's inventory records were so inadequate that the devices would be nearly impossible to track.

39. In the period before Morgan Stanley chose to employ Mr. Oklahoma as a "consultant" and pay him $40,000, he emailed Morgan Stanley that "once I plugged in the shelves, I had access to all of your data that was on the shelves sold to us from a 3rd party. I assume you sold the equipment to someone that sold you their services to destroy data.… If…you sold them without something [like that] in place, you should have at least zeroed out the disks." He added at his deposition that he could use the drives in "any way that he wanted to," and that "if it had enough disks as spares, it would rebuild those volumes and [he] would have access to all that data," referring to all of the Morgan Stanley data that was on the hard drives he had at his disposal. With Morgan Stanley's knowledge and consent, Mr. Oklahoma maintained

unfettered access to those drives for three months before Morgan Stanley retrieved the equipment.

40. A subsequent report on the 2016 Data Center Incident for Morgan Stanley, entitled "Money Movement and JAWS Servers," reflects that those particular servers contained client PII, including client and employee Social Security numbers, passport numbers, and dates of birth. The report further reflects that "the MS Review Team informed us that the data on the [Money Movement Servers and JAWS Servers] was not encrypted or compressed. Therefore, if one of the [hard disk drives] was to be plugged into a computer as an external HDD, the files saved on the HDDs would be visible and could potentially be viewed using a text editor." Virtually every personal computer comes with a text editor pre-installed. And "a SAS HDD controller" which would enable a PC user to read from a Money Movement Server "can be purchased for PCs."

41. Morgan Stanley has identified in discovery at least twenty individuals and entities that purchased equipment containing client PII. Plaintiffs' counsel, in the course of their investigation, located devices sold to one downstream purchaser, contacted that purchaser, and assisted Morgan Stanley in procuring the device. Plaintiffs' expert, who has analyzed the device, has found Morgan Stanley client PII, including the unencrypted PII of one of the named Plaintiffs in this action. Thousands of other devices sold over the internet have yet to be located or recovered.

B. Key Players Involved in the 2016 Data Security Incident

1. Morgan Stanley's Managing Director of Technology and Information Risk (the "Director")

42. The Director led the Morgan Stanley response and investigation effort in the wake of the 2016 Data Security Incident. The Director paid Mr. Oklahoma $40,000 in "consulting

fees" for his silence and promise to wipe the drives, thus deleting the incriminating evidence that Morgan Stanley client data remained on the devices. Despite the Director's knowledge that Mr. Oklahoma had access to Morgan Stanley data, he allowed him to maintain those drives for three months, and made clear that Mr. Oklahoma could use the drives in "any way that [he] wanted to."

43. In his deposition, Mr. Oklahoma was asked, "[s]o as far as you knew, Morgan Stanley was not telling anybody what happened and you were not telling anybody what happened, is that right?" Mr. Oklahoma responded, "I knew I wasn't going to be saying anything. As far as what they wanted to disclose, as they're supposed to, that's on them . . .".

44. Three months after first learning that Mr. Oklahoma had the drives, the Director personally met with Mr. Oklahoma and retrieved the equipment. That same day, the Director received an email from Corporate Security emphasizing that buying Mr. Oklahoma's silence was of utmost importance: "[The] deal with [the] guy is getting a signed [non-disclosure agreement]."

2. Morgan Stanley's Vice President (the "VP")

45. Morgan Stanley's Vice President (the "VP") oversaw the Decommissioning. Morgan Stanley's submissions to the Office of the New Jersey Attorney General reflect its own assessment that the VP "failed to adequately supervise Triple Crown's compliance with its contractual obligations," "failed to validate whether he had received the appropriate certificates [of destruction]," and "failed to appreciate that Triple Crown switched its sub-vendor from the approved sub-vendor (eWorks) to the apparently unapproved sub-vendor (AnythingIT), despite receiving documentary evidence of the change."

46. The VP ignored recognized industry standards with respect to erasing data from the decommissioned equipment, electing to save approximately $100,000 by selecting a non-ITAD vendor for the job, and choosing the "poor man's wipe," which IBM, Morgan Stanley, and

others knew would leave unencrypted data intact on the equipment. When it was explained to him in advance of the Decommissioning that, after the "poor man's wipe," "you can still recover the data from tools until the disks are degaussed," he replied emphatically, "understood!"

47. On October 21, 2019, Morgan Stanley terminated the VP for his failures in oversight of the Decommissioning.

3. Triple Crown Moving and Storage

48. Triple Crown disclosed to the Florida Attorney General that it had no experience with respect to information technology equipment decommissioning. Its website makes clear that it is a moving and storage company.[14] At the time Morgan Stanley engaged Triple Crown, publicly available records reflected that Triple Crown had previously mismanaged storage of another company's electronic equipment.

49. Morgan Stanley classified Triple Crown as a "low risk" vendor and entrusted it with thousands of devices containing unencrypted customer PII.

4. WeedHire/AnythingIT

50. Morgan Stanley worked with WeedHire/AnythingIT both directly and as a subcontractor through Triple Crown throughout the course of the Decommissioning.

51. A 2017 Morgan Stanley Corporate Security and Investigations Report concluded that "[g]iven the scale of the items in the purchase agreement and the firm's debt issues, it was not known if AnythingIT was able to conduct[] its normal business of destroying or clearing IT equipment for resale after April 2016." Yet, as of April 2016, Morgan Stanley was sending WeedHire/AnythingIT unwiped drives with unencrypted data. Morgan Stanley was also selling a large volume of its IT Assets to WeedHire/AnythingIT through its resale auctions.

[14] *See* https://www.triplecrownwarehouse.com/ (last accessed July 2, 2021).

5. IBM

52. IBM is a name synonymous with information technology and security. IBM owned and operated the Poughkeepsie and Columbus data centers, where the Morgan Stanley IT Assets were located. IBM offered to degauss the drives to the Department of Defense ("DoD") industry standard where the "price per drive for sanitization (3x wipe) from IGF is $10." It was not until one day before the first pickup by Triple Crown that Morgan Stanley "decided to use Triple Crown for DS5000 disposition without DOD wiping from [IBM] Lab Services."

6. Stroz Friedberg and PricewaterhouseCoopers

53. In 2018, after realizing the scope and severity of the 2016 Data Security Incident, Morgan Stanley retained forensic expert Stroz Friedberg ("Stroz") and consultant PricewaterhouseCoopers ("PwC") to investigate the Incident. These engagements were directed at minimizing Morgan Stanley's potential liability for and reputational damage from the Incident.

54. Morgan Stanley tasked Stroz with analyzing the equipment it retrieved from Mr. Oklahoma. Having previously paid Mr. Oklahoma approximately $40,000 to overwrite and wipe those drives during the three months that they were in his possession, Morgan Stanley could not have reasonably believed that data remained on them. Still, Stroz found client PII on the equipment, but worked with Morgan Stanley to purportedly disprove Morgan Stanley as the source of that data.

55. Most tellingly, instead of working independently, Stroz solicited comments from Morgan Stanley counsel on its report regarding what Morgan Stanley had called "Project Oklahoma," both orally and in writing, over a period of months prior to issuing that report.

56. Morgan Stanley also engaged PwC to generate reports regarding the 2016 Data Security Incident. PwC and Morgan Stanley maintain a close relationship—at least two members

of Morgan Stanley's Board of Directors are former partners at PwC. Further, an author of the PwC reports assumed a high-ranking position at Morgan Stanley in the weeks following the issuance of two of those reports.

57. The reports themselves further reflect the close relationship—PwC did not conduct an independent investigation. Each report had the same caveat/limitation: "The observations contained herein are based solely on the representations made by the individuals we interviewed, and our analysis of information and documentation provided to PwC. We assume no responsibility for and make no representations with respect to the accuracy or completeness of information provided to us. . . [and] [o]ur procedures and analyses were carried out on the basis that such information and documentation was accurate and complete."

58. PwC's conclusions reveal that PwC did not investigate or discuss any potential causes for the 2016 Data Security Incident except for those that Morgan Stanley provided.

PARTIES

A. Plaintiffs

59. Plaintiffs John and Midori Nelson are citizens of California, residing in Antioch, California. Mrs. Nelson was the primary account holder of a Morgan Stanley IRA account, and Mr. Nelson was the beneficiary. The account was closed on July 14, 2003. On or about July 15, 2020, the Nelsons received Morgan Stanley's Notice of Data Breach, dated July 10, 2020.

60. Plaintiff Sylvia Tillman is a citizen of California residing in San Diego County, California. In the early or mid-1990s, Ms. Tillman signed up for a California Uniform Transfers to Minors Act ("UTMA/CA") account for her minor daughter through Morgan Stanley. Ms. Tillman closed the UTMA/CA account in or about 2000 and has not been a Morgan Stanley client since. Ms. Tillman received Morgan Stanley's Notice of Data Breach, dated July 11, 2020,

on or about that date. The notice specifically stated that the information associated with her UTMA/CA account was exposed by the Data Security Incidents.

61. Plaintiff Mark Blythe is a citizen of Florida residing in Flagler Beach, Florida. In or about 2012, Mr. Blythe signed up for a stock account and an annuity account through Morgan Stanley. On October 3, 2017, Mr. Blythe closed both of his accounts. Mr. Blythe received Morgan Stanley's Notice of Data Breach, dated July 11, 2020, on or about that date.

62. Plaintiff Vivian Yates is a citizen of Florida residing in Riverview, Florida. Ms. Yates established a 529 college savings plan account with Morgan Stanley in or about 2015. That account is still open. Ms. Yates received Morgan Stanley's Notice of Data Breach, dated July 10, 2020, on or about that date.

63. Plaintiffs Richard Gamen and Cheryl Gamen are citizens of Illinois and reside in New Lenox, Illinois. In or about 1989, Richard and Cheryl Gamen established a Morgan Stanley brokerage account. In addition, Mrs. Gamen rolled over her 401(k) individual retirement account to Morgan Stanley. Both the Gamens' accounts were closed in 2010 and 2001, respectively. Mr. and Mrs. Gamen each received Morgan Stanley's Notice of Data Breach, both dated July 11, 2020, on or about that date.

64. Plaintiff Amresh Jaijee is a citizen of New York residing in New York City. Ms. Jaijee signed up for a 401(k) individual retirement account at a Morgan Stanley office in New York in or about 2012. The account is still active. Ms. Jaijee received Morgan Stanley's Notice of Data Breach, dated July 10, 2020, on or about that date.

65. Plaintiff Richard Mausner is a citizen of New Jersey residing in Holmdel, New Jersey. Mr. Mausner had an account with Defendant in New Jersey and closed it no later than

2010. He received Morgan Stanley's Notice of Data Breach dated July 11, 2020, on or about that date.

66. Plaintiff Desiree Shapouri is a citizen of New York and resides in North Hills, New York. Ms. Shapouri had a Morgan Stanley account which she opened in New York in or about 2007. She closed the account in or about 2011. She received Morgan Stanley's Notice of Data Breach, dated July 11, 2020, on or about that date.

67. Plaintiff Howard Katz is a citizen of the Commonwealth of Pennsylvania, residing in Philadelphia. Mr. Katz signed up for his Morgan Stanley trading account in or about the end of 2012. Mr. Katz closed the account in or about 2016. On or about the week of July 20, 2020, Mr. Katz received Morgan Stanley's Notice of Data Breach, dated July 10, 2020.

B. Defendant

68. Defendant Morgan Stanley Smith Barney, LLC is a limited liability company organized under the laws of Delaware, headquartered at 1585 Broadway, New York, New York, with its principal place of business in New York, New York. Morgan Stanley Domestic Holdings, Inc. ("MSDHI"), a corporation organized under the laws of Delaware with its principal place of business in New York, New York, is the sole member of Defendant Morgan Stanley Smith Barney, LLC. Defendant Morgan Stanley Smith Barney, LLC, and its sole member, MSDHI, are both citizens of New York.

69. All of Plaintiffs' claims stated herein are asserted against Morgan Stanley and any of its owners, predecessors, successors, subsidiaries, agents and/or assigns.

JURISDICTION AND VENUE

70. This Court has subject matter and diversity jurisdiction over this action under 28 U.S.C. § 1332(d) because this is a class action wherein the amount in 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 Class Member (including, for example, Plaintiff Sylvia Tillman, a citizen of California; Plaintiff Vivian Yates, a citizen of Florida; Plaintiffs Richard Gamen and Cheryl Gamen, citizens of Illinois) is a citizen of a state different from Defendant.

71. The Southern District of New York has personal jurisdiction over Defendant named in this action because Defendant is headquartered in this District and conducts substantial business in New York and this District through its headquarters, offices, and affiliates.

72. Venue is proper in this District under 28 U.S.C. §1391(b) because Defendant is headquartered in this District and has caused harm to Plaintiffs and Class Members residing in this District.

FACTUAL ALLEGATIONS

A. Background

73. 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 62nd in the 2019 Fortune 500 list of the largest United States corporations by total revenue.

74. Plaintiffs and Class Members are current and former clients of Morgan Stanley living in the United States or abroad with U.S. accounts. They relied on Morgan Stanley 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 have a reasonable expectation that sophisticated financial institutions such as Morgan Stanley will safeguard their PII.

75. Morgan Stanley publicly acknowledges its fiduciary relationship with clients for whom it acts as an investment adviser:

> When acting as your investment adviser, we are considered to have a fiduciary relationship with you. In addition, for advisory retirement accounts, we are acting as a fiduciary under the Employment Retirement Income Security Act of 1974 ("ERISA") and/or under section 4975 of the Internal Revenue Code ("Code").[15]

76. As part of its regular course of business, Morgan Stanley collects and maintains PII from its 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," as well as additional personal identifiers (including passport numbers), mailing and billing addresses, telephone numbers, email addresses, dates of birth, bank account numbers, credit card numbers, and specific asset value and holdings information.

B. The Events of 2016

77. Prior to the mass decommissioning that began in 2014, Morgan Stanley classified the inherent risk of the process as "critical" because the IT Assets contained "Material Non-Public Information" and "PII."

78. Morgan Stanley's ITAD policies required data removal before asset disposal. The policy covered the "end of deployment of a device in its current use" and mandated that all content is removed before [IT Asset] disposal or redeployment." The ITAD Procedure made clear that IT Asset decommissioning was to be performed by authorized personnel or outsourced to a "Security Architecture (SecArch)-approved vendor." The ITAD Procedure further provided that the procedures apply firmwide, and are "intended for all employees and third parties who need to decommission hardware that has been used to carry out Morgan Stanley business."

[15] *See Morgan Stanley Important Account Information*, at 16 (*available at* https://www.morganstanley.com/wealth/relationshipwithms/pdfs/important_account_information.pdf) (footnote omitted) (last visited June 10, 2021).

79. The ITAD Procedure includes examples of compliant IT Asset decommissioning processes for assets that remained operational and were to be disposed or re-deployed, and noted that secure data removal required a "minimum 3x software wipe meeting DoD (Department of Defense) 5520.22M specifications." In addition, the ITAD Procedure required that the BIOS[16] be reset if the asset was to be sent to a third party.

80. In 2014, Morgan Stanley signed an agreement with Triple Crown (the "Consulting Agreement"), a local moving company with no ITAD experience or expertise, for the removal and destruction of approximately 12,000 individual IT Assets. Triple Crown charged Morgan Stanley considerably less money than IBM would have for the job. The Consulting Agreement provided that Morgan Stanley retained "sole discretion" as to whether the disposition of assets was acceptable, and that Triple Crown could "take no action" to dispose of any assets "until and unless" Morgan Stanley granted Triple Crown permission to proceed.

81. The Consulting Agreement provided for certain revenue sharing between Morgan Stanley and Triple Crown. Morgan Stanley negotiated a profit split in which Morgan Stanley would receive 75% of the profits on all of the devices that were resold.

82. Despite the risks associated with reselling used IT Assets containing the PII of millions of Morgan Stanley's clients, the Consulting Agreement incentivized such resale. Destruction of the IT Assets, the preferred and safest method for decommissioning, as reflected in prevailing ITAD standards, was secondary to Morgan Stanley's interest in making a quick profit.

[16] "BIOS" stands for "Basic Input/Output System," defined as "a software element of a computer operating system that allows the CPU to communicate with connected input and output devices." "BIOS.", Merriam-Webster, https://www.merriam-webster.com/dictionary/BIOS (last accessed May 12, 2021).

83. By March 22, 2016, Morgan Stanley decided that IBM, a world leader in information technology as well as the owner of the data centers that housed Morgan Stanley's IT Assets, would not be responsible for wiping Morgan Stanley's equipment and the destruction of its client data during the final stage of the Decommissioning. Morgan Stanley rejected IBM's experience in these tasks opting instead to save costs.

84. Morgan Stanley made a business decision to earn profits from the Decommissioning. On March 21, 2016, two days before the first pickup from the IBM-managed data centers, the VP compiled a cost comparison between Triple Crown and IBM. Morgan Stanley noted that using Triple Crown would represent a savings of $116,867.

85. Despite Morgan Stanley's vendor assessment contemplating the use of Triple Crown only for moving services, Morgan Stanley chose to give Triple Crown full control for ITAD in a hastily arranged project in which Morgan Stanley elected to ignore industry and internal protocols for wiping servers before disposal.

86. Internal Morgan Stanley emails show that Morgan Stanley's plan was to have IBM cease any work related to degaussing of disks and to turn to Triple Crown to provide all disk wipes moving forward.

87. Triple Crown, a moving and storage company, predictably was not familiar with the decommissioning process. On March 29, 2016, after Triple Crown had already picked up hundreds of Morgan Stanley drives with unencrypted client PII, Triple Crown asked Morgan Stanley for clarification "on degaussing vs. erase and re use."

88. Although Morgan Stanley knew that "erase and re use" was not compliant with recognized industry standards and was against written company policy, that was the process it selected for the majority of drives.

89. In addition to Morgan Stanley's failures related to the selected "erase and re use" process, Morgan Stanley exhibited a complete lack of supervision over Triple Crown and its subcontractors throughout the entire process.

90. For example, in the course of the decommissioning process, Morgan Stanley was to receive certificates of destruction ("CODs") for the destroyed IT Assets. These CODs were to serve as confirmation that the IT Assets were destroyed.

91. After Morgan Stanley selected Triple Crown to be the lead vendor on the final stage of the decommissioning project, Morgan Stanley accepted, without protest, bills of lading and Certificates of Indemnification ("COI") from Triple Crown with WeedHire/AnythingIT listed as the consignee. Nowhere on these documents did Triple Crown or WeedHire/AnythingIT state that they had, or were going to, degauss the IT Assets to the DOD standard. Morgan Stanley's corporate representative admitted that "for all the devices we received COIs, we would have no evidence of destruction . . . the [COIs] were not very useful to us."

92. WeedHire/AnythingIT was familiar to Morgan Stanley. In June 2016, Morgan Stanley had contracted directly with WeedHire/AnythingIT "for the resale and disposal of" Morgan Stanley network assets from the Poughkeepsie and Columbus data centers. In fact, WeedHire/AnythingIT picked up devices from the decommissioned data centers.

93. Morgan Stanley's failures in oversight were further highlighted in August 2016 when Morgan Stanley completed a reassessment of Triple Crown. Triple Crown provided updates that contained multiple, written references to WeedHire/AnythingIT. Despite Triple Crown clearly referencing WeedHire/AnythingIT and submitting WeedHire/AnythingIT policies to Morgan Stanley, the review concluded that "[n]o material subcontractors were in scope for

assessment." The Morgan Stanley review ultimately gave Triple Crown a "Control Effectiveness Modifier (CEM): Strong."

94. Morgan Stanley later admitted to the New Jersey Attorney General that the process lacked proper oversight. Morgan Stanley blamed the VP for failing "to appreciate that Triple Crown switched its sub-vendor from the approved sub-vendor (eWorks) to the apparently unapproved sub-vendor (AnythingIT), despite receiving documentary evidence of the change." But internal Morgan Stanley documents reflect that Morgan Stanley not only approved the change, but was actively involved in Triple Crown's use of WeedHire/Anything IT as a sub-vendor.

95. Throughout the course of the Decommissioning, Morgan Stanley recommended and consented to Triple Crown using WeedHire/AnythingIT to assist in the disposal and resale of the data storage devices. Although Morgan Stanley had previous deemed WeedHire/AnythingIT a "high risk" and unsuitable vendor, Morgan Stanley raised no objection to Triple Crown's use of WeedHire/AnythingIT. In fact, Morgan Stanley continued directly contracting with WeedHire for computer asset disposal as well as selling used equipment to them through Morgan Stanley's online auctions.

1. Decommissioned IT Assets Containing Customer Data are Sold on the Internet

96. As a result of the Decommissioning and Morgan Stanley's failure to supervise it, Morgan Stanley's equipment, including unwiped devices containing unencrypted client PII was offered for sale on the internet.

97. With a history of finding its used assets for sale on eBay, Morgan Stanley became aware that its clients' PII was in the hands of unauthorized third parties in October 2017, when

Mr. Oklahoma, an eBay purchaser of used Morgan Stanley IT Assets, initially contacted Morgan Stanley.

98. Mr. Oklahoma sent the email to a legacy internal Morgan Stanley IT email address he found on the used Morgan Stanley equipment his employer had purchased.

99. After Mr. Oklahoma's initial contact, Morgan Stanley requested pictures of labels and serial numbers to prove that the equipment was Morgan Stanley's. Mr. Oklahoma immediately provided unequivocal evidence to that effect.

100. Morgan Stanley did not immediately take steps to retrieve the equipment, or ask Mr. Oklahoma to stop using it. Instead, despite knowing that Mr. Oklahoma and the company he worked for had unfettered access to Morgan Stanley client PII, Morgan Stanley had no further contact with him for six weeks.

2. Morgan Stanley's Lack of Inventory Controls Impedes Its Understanding of What Transpired

101. Morgan Stanley delayed retrieving the drives from Mr. Oklahoma because he was, at its request, attempting to destroy physical evidence of Morgan Stanley's negligence. Morgan Stanley scrambled internally to determine what had transpired, vainly searching records of its relevant dealings with IBM, but taking pains to ensure that its most sensitive internal communications regarding the matter were oral rather than written.

102. As Morgan Stanley tried to account for its decommissioned devices, the consequences of its decision to put profits above all else became clearer. The VP admitted to his colleagues that Morgan Stanley had used asset inventory control software to track decommissioned devices during the early stages of the multi-year decommissioning project. But when the final stage was awarded to Triple Crown, they reverted to using a standard spreadsheet, which had not been properly maintained, updated, or checked by Morgan Stanley during the

process. As a result, Morgan Stanley did not have internal records to verify the disposition of its decommissioned IT Assets.

103. Morgan Stanley's incompetence and lack of documentation was pronounced. On October 31, 2017, the VP asked others at Morgan Stanley whether the drives had been wiped prior to being sent to Triple Crown. Eighteen months after the Decommissioning, the VP did not know who had had responsibility for wiping data from the decommissioned devices.

104. The response received by the VP from the internal Morgan Stanley team speaks volumes: "Had [w]e wiped them, I seriously doubt any records would have been kept. I am pretty sure however that we did not wipe them, … since they were relying on the physical destruction."

105. Another email is tantamount to an admission that Morgan Stanley was noncompliant with its stated decommissioning procedure, with a Morgan Stanley employee admitting: "We do have a deco[missioning] procedure: [] But from the emails I have seen …looks like they wanted a quick recovery, so we only powered down the devices and relied on the degaussing/shred of the items."

106. These internal admissions expose four failures. First, that the drives were not wiped before leaving Morgan Stanley's possession. Second, even if the drives were wiped, Morgan Stanley's tracking process was insufficient to determine what happened to unencrypted drives with client PII. Third, Morgan Stanley IT employees had been operating under the impression that the decommissioned devices were being destroyed, which would have been redundant with data wiping, while Morgan Stanley had entered into an external contract to have the devices resold, which would require wiping. Finally, the VP in charge of the project did not

know what procedures were used and had no documentation to refresh his memory or set the record straight.

107. Internal Morgan Stanley emails show that into November 2017, the VP and others were still unable to confirm whether the drives were wiped. The VP sent an email declaring "there is *no clear recollection or supporting documentation* that confirms any sort of wipes were performed prior to the final/physical decommission stage." Because there was not any.

108. Indeed, there was mass confusion within Morgan Stanley as to whether the decommissioned devices had been destroyed or wiped, and who had been responsible for the wipe. Six weeks after being contacted by Mr. Oklahoma, the Director was still asking for detail on the Decommissioning project. One Morgan Stanley employee responded that "I'm not sure if they were actually wiped by [Morgan Stanley] or if they were remaining on the share before the disks were sent to be destroyed."

109. That same day, another Morgan Stanley employee summed up the decommissioning process failures. In trying to figure out where the process went wrong, he stated, "So guys, is it safe to say that where the [PowerPoint] mentions 'All disks wiped and destroyed' that really means, 'All disks degaussed by vendor, and then destroyed by vendor?'" In short, Morgan Stanley realized at this time that they were wholly reliant on Triple Crown for wiping Morgan Stanley's drives.

110. Morgan Stanley finally began to investigate WeedHire/AnythingIT. On December 7, 2017, The Director noted that the most recent review of WeedHire/AnythingIT was "3 years old, and a fail." That this review was circulated on December 7 was emblematic of Morgan Stanley's bumbling process and lax attitude towards its clients' PII.

111. Pursuant to Morgan Stanley's investigation, the Director asked for documentation concerning Certificates of Destruction ("COD") from WeedHire/AnythingIT associated with the Decommissioning. In response, the VP provided what he called a "COD" for two particular lots associated with the 2016 Data Security Incident. "I'm being told this COD came directly from AnythingIT."

112. The document in question states clearly "Certificate of Indemnification" in large bold letters, rather than "Certificate of Destruction." That Morgan Stanley's then Head of Core Infrastructure, who was eventually terminated along with the VP, could not or would not commit to an answer to the question "[d]o you consider this a COD or COI?" was further evidence of Morgan Stanley's systematic failures in its data security practices.

113. Even into January 2018, Morgan Stanley was trying to find someone else to blame. On January 22, 2018, Morgan Stanley's lax documentation and oversight was further shown when the VP asked IBM for Certificates of Destruction for certain servers. IBM responded that "[i]t's hard to tell what specific [server] you are referring to, but the equipment picked up on 4/22/16 would have gone to Triple Crown for destruction. We would not have any documentation on that." The VP proceeded to claim that "Morgan Stanley paid IBM to do a DOD wipe before TC picked-up this equipment (see attached)." Of course, Morgan Stanley had not.

114. More than two years prior, in a March 2016 email exchange between the VP and IBM employees, the VP discussed a "one pass overwrite" for these devices. IBM cautioned the VP that this was not the DoD wipe that the VP thought it was, and explained that "[t]his was not previously a step we were going to do as [IBM] Lab Services was going to perform the DoD wipe on site in the [Data Centers]." In other words, but for Morgan Stanley's direction, IBM

would have done the industry standard DoD wipe on premises before the assets were picked up. Morgan Stanley opted not to do that.

115. IBM discussed the issue internally, as one manager observed that "[w]hat we do is a very generic pass---data will absolutely be on the drives." IBM went ahead with the generic wipe that Morgan Stanley requested because "IBM is not responsible for ANY equipment after Triple Crown picks it up." Mike Marquardt, the IBM project executive for the data center Decommissioning, added that "I am not sure [the VP] understands what he is buying. . . ."

116. Marquardt's intuition proved correct. On January 22, 2018, the VP sent an email stating that "[p]rior to leaving the POK/COL data centers IBM performed DOD wipes on all the DS5300 SAN. This process was described as a one pass overwrite by recreating RAID arrays on the machine." But a process in which "data will absolutely be on the drives" is not a DoD wipe. It was the process that the VP "understood" would leave data on the drives.

3. Morgan Stanley Initiates Project Oklahoma

117. Almost three months after first learning from Mr. Oklahoma that some of its decommissioned IT Assets containing client data were in his hands, and all the while knowing that Mr. Oklahoma was using the devices at its direction, which would very likely destroy physical evidence, Morgan Stanley decided to retrieve the devices.

118. Morgan Stanley embarked on Project Oklahoma with the legal and compliance team placing the Director at the helm. While outwardly seeming to be a recovery mission for the devices, the effort was an elaborate plan to provide more cover for Morgan Stanley's neglect and failures.

119. Only after internal scrambling, finger-pointing, and confusion did Morgan Stanley contact Mr. Oklahoma, who maintained control and possession of the devices, some six weeks after their previous call.

120. In early December 2017, the Director contacted Mr. Oklahoma using the Director's personal email address, rather than his Morgan Stanley address. The Director asked whether Mr. Oklahoma liked the package the Director had sent him, which included tequila and whiskey. The Director then claimed he "need[ed] to find the break where a vendor sent this down the wrong process and deal with the vendor" even though, by then, it was clear that it was Morgan Stanley's failures that had led to the Incident.

121. Morgan Stanley still could not compile an accurate list of its missing drives, and instead asked Mr. Oklahoma to send Morgan Stanley a list of every drive that he was using.

122. Morgan Stanley requested that Mr. Oklahoma wipe all of the drives he had, and promised that Morgan Stanley would pay him. Mr. Oklahoma performed that work at nights and on weekends, without the knowledge of his employer who had actually purchased the drives, and pursuant to Morgan Stanley's agreement that it would pay him as a "consultant" for his time.

123. On January 21, 2018, three months after Mr. Oklahoma initially contacted Morgan Stanley, and after he thought he had completely wiped the drives at Morgan Stanley's direction, the Director traveled to Oklahoma to pick up the drives. They met at an Oklahoma City location of the restaurant chain Twin Peaks, known primarily for its waitresses' provocative attire, and discussed a draft contract between Mr. Oklahoma and Morgan Stanley, in which Morgan Stanley would pay Mr. Oklahoma $325 per hour for "preparing" the drives for return to Morgan Stanley. Preparing, of course, meant wiping clean. The contract contained a confidentiality provision and provided for Morgan Stanley to pay Mr. Oklahoma's related legal expenses. The Director was clear, "anything you need – I personally guarantee that. My view and [Morgan Stanley's] view is that you helped us out here and we are grateful."

124. The next day, the Director took possession of the now-wiped drives from Mr. Oklahoma at the loading dock at the back of Mr. Oklahoma's place of employment. Mr. Oklahoma confirmed that the plan was for the Director to get to the dock "when nobody else [would] be there." Morgan Stanley and Mr. Oklahoma then executed a contract in which Morgan Stanley agreed to pay Mr. Oklahoma $325 for each hour he spent wiping the Morgan Stanley drives.

4. Morgan Stanley Internally Terms This a "Serious Data Leakage Incident."

125. Six weeks after Morgan Stanley became aware of the IT Assets in Mr. Oklahoma's possession, the Director sent an email marked "high importance" declaring that "[w]e are going to need to pull in someone from WM [Wealth Management] to figure out what was on these disks."

126. Mr. Oklahoma clarified at his deposition in this matter that he could use the drives in "any way that he wanted to," and that "if it had enough disks as spares, it would rebuild those volume and I would have access to all that data," referring to all of the Morgan Stanley data that was on the hard drives he had at his disposal. He maintained unfettered access to that data for the entire time he had possession of the devices, even three months after first contacting Morgan Stanley.

127. A report on the 2016 Data Center Incident for Morgan Stanley reflects that some of the decommissioned servers contained client PII, including client and employee Social Security numbers, passport numbers, and dates of birth. The report further reflects that "the MS Review Team informed us that the data on the [servers] was not encrypted or compressed. Therefore, if one of the [hard disk drives] was to be plugged into a computer as an external HDD, the files saved on the HDDs would be visible and could potentially be viewed using a text

editor." Virtually every computer comes with a text editor pre-installed. And "a SAS HDD controller" which would enable a PC user to read from these servers "can be purchased for PCs."

128. Finally, on January 25, 2018, the Director acknowledged, "[w]e have a problem with one of the storage engineers involved in Oklahoma. Serious data leakage incident." It was only at that point that the Director sought to understand what a nefarious party could do with unwiped, unencrypted equipment, more than three months after confirming that an outsider had its unwiped, unencrypted equipment.

129. Only then did Morgan Stanley begin investigating who might have purchased these devices.

5. Morgan Stanley's Failure to Locate and Secure Additional Missing IT Assets

130. Morgan Stanley identified to Plaintiffs' counsel in 2021 at least twenty individuals or entities that it believed had purchased its IT Assets as a result of the 2016 Data Security Incident. Plaintiffs' Counsel contacted one of those purchasers, who acknowledged that he still had a device in his possession.

131. In September 2016, this individual purchased a NetApp device from Krusecom, the same eBay seller from whom Mr. Oklahoma's employer had purchased.

132. The NetApp device sat for years in this individual's closet, which he described as a "Pandora's box." He lived with several housemates who all worked in the IT field and could have accessed the multiple drives on the device, and the data on the drives.

133. The device has since been recovered from that individual and is in the process of forensic examination. Plaintiffs' expert's preliminary analysis indicates that at least 250,000 unique Social Security numbers are located across the 14 drives, as well as bank account information, names, addresses, telephone numbers, and trading information. And the data clearly belongs to Morgan Stanley and its clients. During preliminary analysis, Plaintiffs' expert found

data regarding one of the named Plaintiffs, including that Plaintiff's full name, address, telephone number, email address, Social Security number, and Morgan Stanley adviser's email address.

6. Morgan Stanley's ITAD Oversight Failure Included Additional Devices

134. On December 14, 2016, a Morgan Stanley employee in the Wealth Management Risk department sent to the Chief Information Security Officer an email entitled "Infosec Projects 2017 v13.pptx." One attachment to this email was a spreadsheet that analyzed PII risk in a variety of different ways. First, Morgan Stanley gave PII a "Risk Rank" between one and five, with five being the most sensitive. Examples of PII that were "Risk Rank" one, or the least sensitive, were client ethnicity, religious affiliations, and sexual orientation. Examples of "Risk Rank" 5, or most sensitive PII, included Social Security numbers, debit/credit card numbers, passport numbers, drivers' license numbers, the three-digit code on the back of the credit card, and tax ID numbers.

135. Next, Morgan Stanley had a list of programs and applications that had the capability of accessing client PII. For every piece of PII that application could access, Morgan Stanley assigned to that application a "points" value that correlated with the "Risk Rank" of the PII at issue. For example: if a hypothetical application could access a client's SSN, Driver's license number, and ethnicity, that application would be given a total "points" value of eleven—five points for the client SSN (risk rank 5), five points for the client's drivers' license number (risk rank 5) and one point for the client's ethnicity (risk rank 1).

136. Morgan Stanley then ranked those applications and programs based on the amount of PII that the program collected. Some applications and programs had access to a full suite of client PII. One such example is the "Web Approvals" application. This application had access to certain data including but not limited to client SSNs, Client Tax ID numbers, Drivers'

license ID numbers, Passport ID numbers, the Client's Full name, address, date of birth, mother's maiden name, and Morgan Stanley login data. In short, this application had enough client PII so that someone could steal identities.

137. Each application was given a unique five-digit "EoN ID," which was used throughout the company to refer to these certain applications. On March 1, 2016, one Morgan Stanley employee in Wealth Management Technology sent to another Wealth Management Technology employee an email entitled "Windows 2003 decom." Attached to the email was a spreadsheet that contained information such as: (1) the name of a server, (2) the location of the server, (3) the type of server, (such as an IBM HS22 blade server with two 146GB hard drives) and (4) the EoN ID applicable to that server. Each server on the list was to be decommissioned and removed.

138. In mid-2018, when Morgan Stanley was investigating its failure to supervise the ITAD process, KruseCom, an eBay reseller of many of the Morgan Stanley devices, sent to Morgan Stanley an asset list of all the Morgan Stanley assets that Krusecom bought from WeedHire/AnythingIT. This asset list contained the name of the server, the type of server, and it identified from which Triple Crown lot the server came. Cross-checking KruseCom's list of servers against Morgan Stanley's list of servers to be decommissioned that contained high risk EON IDs is startling. Against the backdrop of Morgan Stanley's admissions to the New Jersey Attorney General that none of the servers were encrypted, that Morgan Stanley did not wipe the drives on the servers, that WeedHire/AnythingIT did not wipe the servers, and that Krusecom did not wipe the servers, downstream purchasers could have purchased thousands of Morgan Stanley drives with a multitude of sensitive PII, including drives with PII of "Risk Rank" 5.

139. Morgan Stanley's Chief Information Security Officer recognized this. On February 27, 2018, he asked corporate security for a due diligence report on ServerWorlds, explaining that "it appears they are the purchaser of several thousand of the server drives in the Oklahoma incident."

140. Purchase records support the Chief Information Security Officer's suspicions. In April 2016 alone, ServerWorlds purchased 1,600 drives from Krusecom of the size and type that would have fit into the decommissioned server equipment containing client PII.

141. Morgan Stanley then tried to blame others for not wiping its devices. A conversation between WeedHire/AnythingIT and KruseCom, however, summed up the situation quite well: "I don't [l]ike the Morgan [Stanley] witch hunts searching for a reason to place blame. Can you provide the document that they sent you and you sent me that stated that we had to test erase process and provide a data cert for hard-drive wipe[?] (I am not being a jerk but there is none) . . .".

7. Morgan Stanley's Retention of Outside Consultants Was a Whitewash

a. Stroz Friedberg

142. After discovering the 2016 Data Security Incident, Morgan Stanley engaged forensic consultant Stroz Friedberg to analyze the IT Assets recovered from Mr. Oklahoma and several others. Having previously paid Mr. Oklahoma approximately $40,000 to use, overwrite, and wipe those drives, Morgan Stanley could not have reasonably expected that any retrievable data remained on them.

143. Despite Morgan Stanley's efforts to obscure the potential evidence of its malfeasance, a small amount of the drives had not been completely overwritten, and Stroz found some PII belonging to Morgan Stanley clients. Stroz then provided that PII to Morgan Stanley to confirm whether the source of that data was Morgan Stanley, or whether it was mere coincidence

and the data had a different origin. Unsurprisingly, Morgan Stanley returned its results to Stroz in a vindicated form. On October 18, 2018, Stroz completed its report, ultimately concluding that Morgan Stanley was not the source of any data that may have appeared on the drives.

144. This exercise was akin to closing the barn door after the horse was gone, as Mr. Oklahoma and others had been using the drives at Morgan Stanley's direction for several months or more before Morgan Stanley retrieved them. Moreover, Stroz only analyzed the drives after they had been wiped by Mr. Oklahoma, at Morgan Stanley's direction. Yet, Morgan Stanley touted the findings of this report as exculpatory as recently as early 2020.

145. The report in fact proved nothing. The October 18, 2018, review that Stroz produced for Morgan Stanley was severely limited in scope. Of the more than 4,900 known devices that Morgan Stanley contracted with Triple Crown to decommission in 2016, only 246 hard drives were provided to Stroz. Of those 246 hard drives, 73 (nearly 30%) were unsurprisingly wiped and contained no data, making it impossible for Stroz to determine what information may have resided on those drives before Mr. Oklahoma was instructed to spoliate their contents.

146. These 246 devices were grouped by Morgan Stanley—not Stroz—into five tiers based on their respective likelihood of containing client PII, and Stroz searched those drives for a list of patterns and keywords provided by Morgan Stanley.

147. Although some hard drives within those 246 matched Morgan Stanley serial numbers and contained Morgan Stanley client PII, Stroz excluded Morgan Stanley as the source of that information. Stroz provided the Social Security Numbers to Morgan Stanley, and permitted Morgan Stanley to "correlate [] those SSNs with its internal records and for any matches" without any involvement or oversight from Stroz, waited for Morgan Stanley to

provide keywords like account numbers, names, and addresses associated with those Social Security Numbers, and then, because other data elements were associated with those Social Security Numbers—such as credit card numbers and other bank account information that Morgan Stanley purportedly did not collect—ruled out Morgan Stanley as the source of that data. But another consultant reported that bank account and financial account information was collected and stored by Morgan Stanley.

148. Most tellingly, Stroz solicited comments from Morgan Stanley counsel on its report regarding Project Oklahoma, both orally and in writing, over a period of months prior to issuing its report.

b. PricewaterhouseCoopers

149. On or about April 30, 2018, after realizing the scope and severity of the 2016 Data Security Incident, Morgan Stanley engaged PwC to analyze all available information regarding the presence of Morgan Stanley client PII on several different categories of IT Assets subject to the 2016 Data Security Incident, comprising over 100 servers and thousands of individual hard disk drives ("HDDs") that Morgan Stanley determined had already been sold to outside vendors. PwC's work for Morgan Stanley was conducted between April 30, 2018 and October 15, 2019.

150. The scope of this investigation was limited to information that Morgan Stanley provided to PwC; in other words, PwC conducted no independent investigation of its own. In fact, PwC solicited Morgan Stanley's comments on those reports just prior to their issuance, and at least one of the authors of the PwC reports joined Morgan Stanley as an executive just weeks after two of the reports were delivered.

151. In its series of five reports, PwC qualified its analysis with the fact that PwC had no knowledge regarding whether anyone had read or otherwise accessed the data left on the

drives. For the drives that PwC identified as being readable without any mitigating controls, PwC took great pains to explain that the PII that was ostensibly on those devices did not contain any Social Security or passport numbers. For those drives that may have nonetheless contained sensitive PII, PwC explained that an actor would either need a connection not frequently found in PCs, or that there was not enough information available for PwC to analyze whether an actor could have rebuilt the drives.

C. Morgan Stanley Refuses to Acknowledge Its Own Failures

152. In December 2017, in the midst of Morgan Stanley learning that its decommissioned assets containing customer PII had been auctioned for sale on the internet and in the wake of the stark realization that it had no inventory control management system, the Director reported to his bosses that with regards to "control testing," Morgan Stanley had made "considerable improvements in the last year . . . ." The documents provided by the Director in support of this statement show that Morgan Stanley's failure to follow its own protocol to destroy decommissioned assets and failure to wipe data from devices that were not destroyed had existed for some time.

153. The risk description in one Risk Register document stated that: "A sample of 45 servers decommissioned between October 2014 and May 31, 2015 were selected to confirm that the data was wiped or degaussed . . . [w]e were unable to evidence that a select number of devices had been previously 3x wiped or OS/Rebuilt as applicable." The Risk Register was clear: "The risk of not having evidence maintained could result in missing/misplaced HDDs with confidential/high sensitive data not being appropriately and timely degaussed . . . ."

154. Another Risk Register document from 2015 identified the risks that materialized during the mass decommissioning: "Final disposition of assets is not made available as part of the IT asset decommissioning request process, resulting in the Enterprise Data Center (EDC) and

global Alchemy teams' inability to maintain an inventory to track disposition attributes . . . of decommissioned assets . . . ." This document also referenced the random sampling discussed in Risk Register RSK-1407. "For 28 out of 45 samples selected, we were unable to determine that a validation or tracking is performed throughout the process among the teams."

155. In two different places, Morgan Stanley admitted that its ineffectual processes could expose client PII. The Risk Register states, "[t]he risk of not having a complete and regularly updated inventory containing the list of HDDs detached from their respective servers could result in missing/misplaced HDDs with confidential/high sensitive data not being appropriately and timely degaussed increases the risk that firm information could be exposed and compromised." Even more prescient, the Register later stated, "confidential/high sensitive data that was stored on the device could be recovered using the appropriate tools."

D. The 2019 Data Security Incident

156. Morgan Stanley did not learn any lessons from the 2016 Data Security Incident and continued repeating its own errors.

157. In 2019, Morgan Stanley disconnected and replaced approximately 500 Cisco WAAS Servers in local branch offices pursuant to a larger program to refresh its computer hardware. Morgan Stanley hired ITAD vendor Arrow to conduct the decommissioning of these devices. Later that year, Arrow notified Morgan Stanley that it would no longer provide these ITAD services. During the wind-down period of Morgan Stanley's dealings with Arrow, Morgan Stanley undertook a cross-check and reconciliation of its records of the devices it understood were provided to Arrow for data destruction. During that review, Morgan Stanley discovered that WAAS Servers were missing.

158. Despite being on notice of the risks that await an entity that fails to sanitize customer PII from its IT Assets before disposing of them or transferring them, Morgan Stanley

did not learn from its prior mistakes, and transferred the WAAS Servers to Arrow with the client data contained on them largely intact and accessible.

159. Additionally, because Morgan Stanley failed to maintain proper chain of custody records of the location of the WAAS Servers, and failed to verify the sanitization of customer data from those servers, Morgan Stanley again found itself in the same position as it had been in only two years earlier—in breach of all applicable standards of care owed Plaintiffs and Morgan Stanley's millions of other clients regarding the protection of their most sensitive PII from disclosure.

160. In February 2020, the Morgan Stanley team responsible for overseeing the WAAS Servers, reported to the company that the devices were missing based on its inventory review.

161. Having failed again to follow applicable ITAD standards of care regarding the WAAS Servers, Morgan Stanley was nevertheless able to recover these servers on or about February 28, 2020.

162. On July 31, 2020, following its recovery of the WAAS Servers, Morgan Stanley again engaged Stroz to perform analysis of the servers, and in furtherance of that engagement, drafted a memorandum on its analysis and submitted it to Morgan Stanley on or about July 31, 2020, approximately three weeks after Morgan Stanley had already begun notifying Plaintiffs and members of the Class about the 2019 Data Security Incident.

163. Stroz's analysis was geared at both identifying any Morgan Stanley client PII stored on the relevant IT Assets and assessing the accessibility of that PII to those who might want to extract it.

164. Specifically, Stroz conducted patterned searches for the following categories of PII:

a. Social Security numbers;

b. credit card numbers;

c. credit card number Track 2 information;

d. telephone numbers;

e. URLs;

f. email addresses;

g. IP addresses;

h. network-related data;

i. http web request logs; and

j. Windows shortcut files and Windows file references.

165. Those searches yielded over 2,000 hits for Social Security numbers across the six WAAS Servers and Stroz identified over 1,400 corresponding records remaining on the servers capable of being reconstructed to identify individuals associated with these numbers. Moreover, the foregoing keywords generated thousands of additional results across the sectors of the WAAS Servers searched by Stroz.

166. Morgan Stanley, after learning that its client data potentially remained on the WAAS servers after their disposition by Arrow, contacted Cisco to better understand how the WAAS Servers' encryption function and data sanitization "wipe" function "actually worked." Based on its understanding of the Cisco summary of the servers' functionality, Stroz concluded that the WAAS Servers' data "wipe" function did not actually wipe data. Furthermore, according to the summary, when the encryption function of the servers is enabled, data is merely partitioned off from newly encrypted data and not actually encrypted.

167. After conducting its analysis of the WAAS Servers and evaluating Morgan Stanley's audit of those Servers' functionality, Stroz ultimately concluded, consistent with Cisco's explanation to Morgan Stanley:

> From our review, it appears, that the "wipe" function does not forensically wipe data but merely creates a new partition in place of a prior partition. Stroz Friedberg also observed that enabling encryption, again consistent with Cisco's explanation, encrypts only new data, while leaving data from the previously existing partition on the disk in a manner that is recoverable using forensic tools.

168. This software flaw highlights the importance of following proper ITAD procedures. The fact that the 2019 Data Security Incident transpired after the 2016 Data Security Incident and PwC's audit shows Morgan Stanley's disregard for the safety of client PII. The Stroz report accurately details all of the shortcomings in Morgan Stanley's oversight that resulted in the 2019 Data Security Incident. Had Morgan Stanley had an accurate inventory of its IT Assets, this situation could have been avoided.

E. The Scope of the Data Security Incidents is Substantial

169. Morgan Stanley engaged PwC to analyze information regarding the presence of Morgan Stanley customer PII on several different categories of IT Assets, comprising over one hundred servers and thousands of individual HDDs that Morgan Stanley determined had already been sold to third party vendors. PwC's work concluded with the preparation of five reports.

170. Included in these reports were: (a) Morgan Stanley's own assessment of the "Root Cause Issues" of the event in which it admitted to multiple breaches of the applicable standard of care over the entire ITAD process across its corporate structure; and (b) detailed assessments of the accessibility of the several highly sensitive and valuable categories of customer PII remaining on the several different types of IT Assets subject to the 2016 Data Security Incident.

171. The scope of PwC's analyses of Morgan Stanley's IT Assets for all five reports was the same: whether someone in possession of some or all of the foregoing server equipment

could access data and read information saved on any of those servers' associated HDDs. After spending time interfacing with individuals from Morgan Stanley's Wealth Management Technology and Enterprise Technology and Risk teams (the "MS Review Team"), and other personnel responsible for the oversight and maintenance of certain categories of these assets, PwC concluded that across IT Asset categories, comprising thousands of individual HDDs containing Morgan Stanley PII of over 14 million individuals, third parties would be able to access some or all of that data if in possession of the right combination of those IT Assets.

172. Perhaps more startling than the number of current and former Morgan Stanley customers whose data was revealed to now be accessible by thieves, PwC's analyses also revealed the breadth of sensitive PII stored by Morgan Stanley on these assets that, upon information and belief, found its way into the hands of criminals to the ultimate injury of Plaintiffs and Class Members. PwC's analyses also revealed that much of this PII had not been encrypted by Morgan Stanley or, as determined by the Morgan Stanley Review Team for certain categories of assets, there were no then-existing mitigating controls or protocols designed to remove that PII at the time Morgan Stanley transferred the assets to Triple Crown.

173. Indeed, prior to the transfer to Triple Crown, the following IT Assets that were the subject of PwC's analyses contained vast amounts of PII and other confidential information about Morgan Stanley's current and former clients that would be valuable to criminals:

a. "CMAT Servers" – customer account information, trader account numbers, trader IDs, sales person IDs, and customer transaction details, including security IDs, trade dates, buy/sell indicators, trade quantities, trade prices and settlement dates;

b. "LDAP Servers" – employee first, middle, and last names, home addresses, mobile phone numbers, month and date of birthday, last four digits of Social Security number, and company password history;

c. "Call Center Agent Scheduler IEX Server" – Morgan Stanley Call Center Agent and Supervisor information, including names, phone numbers, email addresses and employee IDs;

d. "FID Servers" – employee email addresses and employee IDs;

e. "FIX Appia Servers" – employee names and trade order transaction information, including symbols, quantities, buy/sell indicators, price, and timestamp;

f. "Minerva App Servers" – customer first and last names, Morgan Stanley trader first and last names, user IDs, customer and employee email accounts, customer account numbers, and trade order transaction information, including symbols, quantities, buy/sell indicators, price, and timestamp;

g. "Hadoop Servers" – customer account numbers and IDs, names, birth years, household IDs, addresses, transaction amounts, and status as a PC user; Morgan Stanley Financial Advisor branch number, user ID, name, employee ID and employment status; and customer transaction and portfolio position details, including trade dates, settlement dates, buy/sell codes, prices, trade quantities, position quantities and market values;

h. "Money Movement Servers" – customer account numbers, account owner names, external account owner names, payee names, payee mailing addresses, customer names and addresses, external client bank names, routing and account numbers, Morgan Stanley bank account numbers, customer IDs, and transaction amounts; and

i. "JAWS Servers" – customer names, nicknames, genders, marital status, dates of birth, addresses, home and office phone numbers, account numbers date of death, Social Security numbers, passport numbers, issue countries and dates of expiration, and employee Social Security numbers and Financial Advisor numbers.

174. In its reports, PwC also makes explicit reference to the fact that according to Morgan Stanley, the client PII remaining on the Money Movement, JAWS, Hadoop, Call Center Agent Scheduler IEX, FID, FIX Appia, and Minerva App Servers at the time those assets were transferred to Triple Crown, was not encrypted, and instead was maintained as accessible text on those assets.

F. Morgan Stanley's Investigation Exposes the Failure of the ITAD Process.

175. Subsequent to learning that a large volume of its client PII had not been properly encrypted or sanitized and that there were thousands of unaccounted for IT Assets, Morgan Stanley conducted its own audit of the IT Asset decommissioning process that led to the 2016 Data Security Incident. The investigation documented the "root cause issues" of and extent of its failure over the entire ITAD process across its corporate structure and specifically in the areas of: (a) leadership and responsibility; (b) vendor management; and (c) risk management. Following this audit, on October 15, 2019, PwC submitted its fifth and final report to Morgan Stanley on the Data Center Incident: "Project Oklahoma Analysis of Root Cause Issues and Related Recommendations." In this report, PwC provided recommendations on Morgan Stanley's own recommended remediation of its IT Asset decommissioning program following the identification of these "root cause issues."

176. First, Morgan Stanley determined that neither key stakeholders in senior management nor members of its Enterprise Infrastructure, Wealth Management, and Technology Information Risk groups "sufficiently asserted or exercised full ownership over data

commissioning, as distinct from application migration" for the decommissioning project at the heart of the Data Security Incident. According to Morgan Stanley, "this resulted in a failure to receive reporting on and exercise senior oversight over the successful execution of data destruction, as well as a failure to prioritize and effectively manage risks on key decisions such as potential asset resale, the selection of the decommissioning vendor, and accelerated decommissioning procedures for the devices in the Poughkeepsie and Columbus data centers."

177. Morgan Stanley determined that the failure at the executive level to properly manage the decommissioning of these two data centers carried over to its lower-level employees, as well. It found that multiple individuals responsible for data decommissioning generally "expressed uncertainty over the organizational responsibility for, and policies and procedures governing decommissioning" during the decommissioning of the two data centers. Morgan Stanley, likewise, concluded that employees directly responsible for the decommissioning of IT Assets "appeared disconnected from [Morgan Stanley] leadership, and there was an unclear supervisory chain for those employees such that no one directed and established appropriate expectations, oversight, and accountability for the . . . decommissioning process."

178. Morgan Stanley's audit also determined that its ITAD vendor management protocols were deficient, revealing a disconnect between vendor selection and "the 'business' on the ground." Further, it established that Morgan Stanley recklessly ran afoul of governing ITAD standards in the three following ways:

a. its supplier risk management process "failed to identify certain risks related to the Triple Crown vendor relationship (because, for example, it did not distinguish Triple Crown from [its previous ITAD partner] or evaluate it separately, or ensure that risks were

communicated and considered by business contacts throughout the organization that continued to use Triple Crown)";

b. "[t]here was no clear ownership of the Triple Crown relationship, and the personnel directly working with the vendor on the ground lacked knowledge of or disregarded key contractual provisions, which led to the ineffective oversight and management of the Triple Crown relationship"; and

c. "[t]here was a lack of clarity concerning, and diligence over, the permitted resale of decommissioned assets and allocation of proceeds."

179. Finally, Morgan Stanley's own audit found that Morgan Stanley "inadequately assessed or addressed the significant risks posed by any data potentially on the devices being decommissioned." This critical violation of the applicable standard of care demonstrated Morgan Stanley's careless, reckless, and negligent disregard of the privacy of Plaintiffs and members of the Class, leading to:

a. "the failure to require reporting to the [Morgan Stanley] steering committee through the completion of decommissioning";

b. "the failure to follow Morgan Stanley's risk management processes with respect to decommissioning . . . ";

c. "the failure to ensure that devices containing data were wiped or physically destroyed prior to Morgan Stanley surrendering control over them"; and

d. "the failure to ensure diligent assessment of sensitive data on the assets prior to decommissioning."

180. Additionally, Morgan Stanley found there was both insufficient tracking of the IT Assets that were the subject of the 2016 Data Security Incident, and insufficient documentation

relating to data destruction on those assets. Finally, Morgan Stanley determined that "[t]he relevant personnel on the ground failed to manage risk because they ineffectively monitored Triple Crown's contractual performance, and failed to notice key events that should have alerted them to the developing non-compliance with the relevant contract and Morgan Stanley policies (such as the fact that Triple Crown started sending [Certificates of Indemnification] from AnythingIT rather than [Certificates of Destruction] from [Triple Crown's former ITAD partner])."

181. Morgan Stanley's own assessment of the multitude of errors it committed throughout the Decommissioning of the Poughkeepsie and Columbus data centers reveals a stark through line of recklessness that infected the company's entire understanding and administration of ITAD issues, resulting in multiple breaches of the standard of care owed to Plaintiffs and Class Members.

182. Morgan Stanley failed to perform proper due diligence and exercise control over the chain of custody of IT Assets, failed to perform proper data sanitization on those assets, and then lost track of those assets in the recycling process. These compounding failures on the part of Morgan Stanley demonstrate a shocking level of disregard for the privacy interests of its customers. It is also a textbook illustration of complete non-compliance with the NIST and related ITAD standards set forth herein.

183. Following Morgan Stanley's identification of the root causes of the 2016 Data Security Incident, it implemented several remedial revisions to existing ITAD policies to purportedly address its failure to adhere to governing ITAD standards before, during, and after the closure of the New York and Ohio data centers. In PwC's Project Oklahoma Analysis, it both chronicled Morgan Stanley's ITAD remedial actions in the wake of the Data Security Incident,

and provided recommendations to Morgan Stanley regarding internal remediation steps to be taken to address the event's root causes.

184. PwC included in its Project Oklahoma Analysis eighteen recommendations to Morgan Stanley that PwC believed would enhance Defendant's own remediation of its ITAD policies. These recommendations follow the data sanitization, ITAD vendor chain of custody verification, and risk management recommendations of NIST and those followed globally by ITAD professionals.

185. The import of PwC's Project Oklahoma Analysis of Morgan Stanley's audit of the 2016 Data Security Incident is clear: at all times relevant to the Decommissioning of the Poughkeepsie and Columbus data centers, there existed voluminous authoritative industry standards for IT Asset sanitization and disposal that should have governed the decommissioning of those data centers but did not. This was exclusively due to Morgan Stanley's negligence that ultimately was the direct and proximate cause of the 2016 Data Security Incident and the resulting injuries to Plaintiffs and Class Members.

G. Morgan Stanley's Assessment of the Dark Web was Belated and Intentionally Insufficient

186. In November 2020, Morgan Stanley requested that Flashpoint, Inc. search the dark web for Morgan Stanley client information. This timing is significant—by this point Morgan Stanley had: (1): told multiple Attorneys General that Morgan Stanley had no reason to think that client information had been accessed, (2) had been fined by the OCC, and (3) been on notice of Plaintiffs' initial complaint.

187. To compound the dilatory nature of Morgan Stanley's perfunctory effort, Morgan Stanley designed Flashpoint's search protocol to be overly narrow in scope, as to intentionally obstruct Flashpoint's investigation.

188. Morgan Stanley directed Flashpoint to search for "Morgan Stanley customer information." When Flashpoint asked for clarity as to what was included in that definition, Morgan Stanley responded in bold, that it was PII "for individuals explicitly identified as being Morgan Stanley clients (e.g., 'tax records for sale for Person A, a client of Morgan Stanley')." When Flashpoint tried to expand the breadth of its search to make it more comprehensive, Morgan Stanley again limited the scope. "Please limit your search to Morgan Stanley rather than other acquired or affiliated entities."

189. These limitations are significant, particularly given Morgan Stanley's merger with Smith Barney. On October 25, 2017, the day that Morgan Stanley received the email from Mr. Oklahoma, Morgan Stanley was trying to analyze the NetApp assets that were in the Poughkeepsie and Columbus data centers. At that time, Morgan Stanley stated, "[w]e do not have many breadcrumbs about these arrays since they came with the [S]mith [B]arney merger . . . ." Thus, IT Assets in the Poughkeepsie and Columbus data centers included devices that had belonged to Smith Barney.

190. In any event, it is unclear that broadening the search to include Smith Barney would even help, as dark web threat actors frequently do not identify the source of a data breach. Morgan Stanley knows this well. Unrelated to the engagement described above, Morgan Stanley hired Flashpoint to acquire a database advertised to have names and passwords from a "US Financial firm." Morgan Stanley had Flashpoint pay the hackers to acquire the database so that Flashpoint could assess whether Morgan Stanley information was included, as the seller did not identify the source of the information.

H. State Attorneys General Investigations

191. Beginning in July 2020, Morgan Stanley began responding to several states Attorneys General inquiries regarding both the 2016 and 2019 Data Security Incidents. In letters

and related responses about both Incidents to and from at least nine Attorneys Generals, Morgan Stanley made several admissions. The letters obfuscate the impact of both Incidents.

192. Morgan Stanley's letters to state Attorneys General from July through October of 2020 include several inconsistent, incomplete, and contradictory representations. For example, on July 10, 2020, Morgan Stanley sent a letter to the Connecticut Attorney General regarding what it described as "*potential* data security incidents." As set forth herein, Morgan Stanley knew there was nothing "potential" about either of the Data Security Incidents.

193. Similarly, Morgan Stanley's representation to the Arkansas Attorney General on September 8, 2020, that it "*immediately* took steps" to recover IT Assets from the 2016 Data Security Incident and initiated "wide ranging investigation and recovery effort," conflict with the wealth of documents and testimony Plaintiffs have adduced to date. Morgan Stanley's dilatory and highly secretive dealings with Mr. Oklahoma, as well as its limited and incomplete efforts to track down the IT Assets in question, contradict Morgan Stanley's position.

194. Morgan Stanley represented to the Colorado Attorney General on September 8, 2020, that it submitted an insurance claim under its cyber liability policy relating to the 2016 Data Security Incident on February 6, 2018, which was two-and-a-half years before Morgan Stanley alerted its clients about the Incident. This demonstrates an egregious breach of the standard of care owed to its clients to protect their PII. Indeed, between 2018 and 2020, and unbeknownst to Plaintiffs and Class Members, third parties were already in possession of their PII. Morgan Stanley's failure to timely notify its clients about the Incident impeded them from being in a position to immediately address the harm resulting therefrom.

195. Morgan Stanley's inconsistent, contradictory, or incomplete responses highlight its attempt to evade responsibility for its repeated failures involving its ITAD practices. For

example, the October 2018 Stroz report stated that Morgan Stanley had identified 78 of the drives analyzed as formerly belonging to Morgan Stanley. But two years later in August 2020, Morgan Stanley reported the same number to the Florida Office of the Attorney General. That disclosure neglects to mention that Morgan Stanley had been unable to identify a single additional drive in the two years following the Stroz report, or that the 78 drives identified were from the first batch of 246 hard drives that Morgan Stanley acquired and analyzed. Indeed, after merely a "months-long investigation, the Firm concluded that there was no reason to believe that there [had] been any unauthorized access to or unauthorized acquisition of computerized data containing personal information."

I. Morgan Stanley Enters Into a Consent Order with the OCC.

196. The OCC determined that Morgan Stanley "was in noncompliance with 12 C.F.R. Part 30, Appendix B, 'Interagency Guidelines Establishing Information Security Standards,' and engaged in unsafe or unsound practices that were part of a pattern of misconduct." Consent Order, § II(5).

197. The relevant regulation requires Morgan Stanley to maintain client information for only five years after any activity related to an account. *See* 17 C.F.R. § 275.204–2(e)(1). Instead of destroying personal and sensitive financial data at that point, Morgan Stanley amassed enormous volumes of data without properly encrypting and physically securing it, which only enlarged the size of the class and cumulative damage to Plaintiffs and the Class.

198. Beginning on or about July 9, 2020, at the direction of the OCC, Morgan Stanley sent customers a "Notice of Data Breach." In this notice, Morgan Stanley informed the victims of the 2016 Data Security Incident 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.[17]

199. On or about July 10, 2020, Morgan Stanley sent notifications of the Data Security Incidents to various state attorneys general, including Iowa Attorney General Tom Miller. That notification reported the 2016 Data Security Incident and added information about the 2019 Data Security Incident:

> 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.[18]

200. Morgan Stanley admitted that the hardware involved in both the Data Security Incidents "left our possession" containing unencrypted information, and "it is possible that data associated with [clients'] account(s) could have remained on some of the devices when they left our possession."[19]

201. Morgan Stanley further admitted that the unencrypted PII that "left [its] possession" included information from clients and any "individual(s) associated with [clients'] 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."[20]

---

[17] ECF No. 11, at 1.

[18] *See Letter to Iowa's Attorney General Tom Miller*, dated July 10, 2020, a true and correct copy of which was filed as ECF No. 1-2.

[19] ECF No. 1-2.

[20] ECF Nos. 1-1, 1-2.

202. For UTMA/CA accounts, for example, the lost PII would include the PII of custodians managing the accounts as well as the minor account holders.

J. Morgan Stanley Owed a Duty To Its Customers

203. Morgan Stanley's duty to adopt, implement, and maintain reasonable security measures to protect its clients' PII arose as a result of the special relationship that existed between Morgan Stanley and Plaintiffs and the Class. That special relationship arose because Plaintiffs and the Class Members entrusted Defendant with their confidential PII, which Morgan Stanley required that they provide in order to open and maintain their accounts with the company.

204. In addition, Morgan Stanley publicly acknowledges its fiduciary relationship with clients for whom it acts as an investment adviser.[21] Those clients thus had good reason to believe that Morgan Stanley would comply with financial industry standards governing the security of client data. Its above-referenced "Privacy Pledge" and U.S. Customer Privacy Notice explicitly state as much.[22] A page on the Morgan Stanley website addressed to online security likewise represents: "At Morgan Stanley, safeguarding your assets and personal information is among our highest priorities."[23]

205. That fiduciary relationship required Morgan Stanley to promptly notify victims of the 2016 Data Security Incident upon learning of it in late 2017. Morgan Stanley was aware of the urgency of that notification. Morgan Stanley Wealth Management's Head of Data Protection

---

[21] *See Morgan Stanley Important Account Information*, at 16 (*available at* https://www.morganstanley.com/wealth/relationshipwithms/pdfs/important_account_information.pdf) (last visited June 10, 2021).

[22] *See supra* ¶¶ 4-5.

[23] See https://www.morganstanley.com/what-we-do/wealth-management/online-security (last visited May 18, 2021).

and Infrastructure Risk disclosed in 2019 that "[f]or the last two years, cybersecurity and identity theft has been the number one concern of our clients."[24]

206. Morgan Stanley was subject also to an "independent duty," untethered to any contract between it and Plaintiffs and members of the Class, to safeguard their PII.

207. Furthermore, Morgan Stanley also had a duty to adopt and exercise appropriate clearinghouse practices to remove the PII of former account holders that Morgan Stanley was no longer required to retain pursuant to applicable law.

208. Finally, Morgan Stanley maintained a statutory duty, pursuant to New York General Business Law § 899-aa, which requires "[a]ny person or business which owns or licenses computerized data which includes private information" to disclose "any breach of the security of the system following discovery or notification of the breach in the security," including such instances in which private information is "*acquired by a person without valid authorization*." *Id.*, § 899-aa(2) (emphasis added).

K. Morgan Stanley's Conduct Violated Regulatory Guidelines and Industry Standards

1. Morgan Stanley Failed to Comply with FTC Guidelines

209. Federal and State governments have likewise established security standards and issued recommendations to temper data breaches and the resulting harm to consumers and financial institutions. The Federal Trade Commission ("FTC") has issued numerous guides for business highlighting the importance of reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.[25]

[24] "Cybercrime Is the New Organized Crime | Morgan Stanley Minute," available at https://www.youtube.com/watch?v=zkazfXU-R0Q (last accessed June 16, 2021).

[25] Federal Trade Commission, *Start With Security, available at* https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf

210. In 2016, the FTC updated its publication, "Protecting Personal Information: A Guide for Business," which established guidelines for fundamental data security principles and practices for business.[26] The guidelines note businesses should protect the personal customer and consumer information that they keep, as well as properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct security problems.

211. The FTC recommends that companies verify that third-party service providers have implemented reasonable security measures.[27]

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

213. Morgan Stanley was at all times fully aware of its obligation to protect the personal and financial data of its clients, including Plaintiffs and Class Members. Morgan Stanley was also aware of the significant repercussions if it failed to do so.

214. Morgan Stanley's failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data—including Plaintiffs' and Class Members' Social Security numbers, dates of birth, and other highly sensitive and

[26] Federal Trade Commission, *Protecting Personal Information: A Guide for Business, available at* https://www.ftc.gov/tips-advice/business-center/guidance/protecting-personal-information-guide-business

[27] FTC, *Start With Security, supra* note 5.

confidential information—constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45

2. Morgan Stanley Violated ITAD Industry Standards.

215. Widely accepted industry standards govern the sanitization and disposal of the IT Assets. Over the course of events precipitating, during and following the Data Security Incidents, Morgan Stanley repeatedly violated those standards, leading to the disclosure of millions of its clients' most confidential PII.

216. According to Gartner, Inc. ("Gartner"), a leading IT research and advisory firm that advises over 14,000 entities in over 100 countries, the three most important aspects of IT asset disposal are: transportation logistics (including chain of custody), data sanitization, and recycling.[28]

217. To minimize chain of custody security risks, Gartner recommends that ITAD managers, especially in the healthcare and financial sectors, require that some form of data sanitization be performed on-site prior to disposal.[29] Gartner further recommends that entities not requiring on-site data sanitization, should "at a minimum enforce data encryption on all data-bearing devices to minimize chain of custody security risks."[30] And for those organizations who leave data sanitization to outside vendors, Gartner recommends that the data be sanitized according to prevailing ITAD industry standards, such as those promulgated by the United States National Institute of Standards and Technology ("NIST").[31] As made clear above, Morgan Stanley did not meet the requirements.

---

[28] See Ex. A, at 5.

[29] *Id.* at 6.

[30] *Id.*

[31] *Id.* at 5-6.

218. NIST, empowered by the Federal Information Security Management Act of 2002, 44 U.S.C. § 3541 et seq., is responsible for developing information security standards and guidelines for federal information systems, but its widely available ITAD standards on media sanitization were designed for use by all public and private organizations in the United States. According to one experienced ITAD vendor, NIST is "the go-to data erasure standard in the United States."[32] Indeed, according to NIST's December 2014 Special Publication 800-88, "Guidelines for Media Sanitization," once an entity makes the decision to decommission IT assets and sanitize data from them, that entity must undertake a series of decisions to ensure: (a) that proper methods of data sanitization will be employed and (b) proper verification of data sanitization and IT asset disposal, including capturing decisions and actions of all relevant actors and interfacing with key officials.[33]

219. NIST recommends that organizations undertaking asset sanitization and decommissioning:

a. verify the selected information sanitization and disposal process by using one of two types of verification: verification every time data sanitization is applied or employment of representative sampling verification, applied to a selected subset of the media;

b. verify the integrity of sanitization tools used for media sanitization prior to beginning data sanitization (e.g., a degausser or a dedicated workstation, proper equipment calibration, testing, maintenance);

---

[32] *See* https://ld7un47f5ww196i744fd5pi1-wpengine.netdna-ssl.com/wp-content/uploads/2018/08/data-sanitization-in-the-modern-age-dod-or-nist.pdf (Last visited May 13, 2021).

[33] *See* NIST, "*Guidelines for Media Sanitization*", Special Publication 800-88, December 2014, at 19, available at https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-88r1.pdf. (Last visited May 13, 2021).

c. verify the level of expertise of the personnel performing media sanitization to ensure they are competent to perform sanitization functions;

d. verify the results of media sanitization for all IT assets subject to sanitization if those assets are to be recycled and used by another user following disposition; and

e. certify the disposition of all media following sanitization for every IT asset that has been sanitized.[34]

220. Consistent with the recommendations of Gartner, NIST, and the International Association of Information Technology Asset Managers, Inc. ("IAITAM"),[35] it is of paramount importance to sanitize IT assets before an entity seeking to retire such assets provides them to a vendor for disposal or recycling.[36]

221. Consistent with the NIST standards, IAITAM recommends that entities employ sufficient verification throughout the IT asset disposal process to ensure that evidence of chain of custody of IT assets and corresponding data destruction is "reliable, verifiable and unimpeachable."[37] Therefore, according to the IAITAM, "verification cannot be outsourced to the disposal vendor or delegated to the same employee responsible for physically performing ITAD activities."[38]

---

[34] *Id*. at 20.

[35] *See* https://iaitam.org (Last visited May 13, 2021).

[36] Robert Johnson and Kyle Marks, *Data Breach Prevention Driver for Disposal*, ITAK, May 26, 2014, available at https://itak.iaitam.org/data-breach-prevention-driver-for-disposal-it-asset-disposition-diligence-starts-day-one-2/ (Last visited May 13, 2021).

[37] Kyle Marks, *Consider ITAD a Security Incident*, ITAK, April 27, 2013, available at https://itak.iaitam.org/consider-itad-a-security-incident-a-practical-look-at-itad-security-issues-2/ (Last visited May 13, 2021).

[38] *Id.*

222. Morgan Stanley, during its internal audit of the 2016 Data Security Incident, concluded that it had failed to adhere to the foregoing standards governing the decommissioning of IT Assets. Instead, Morgan Stanley followed outdated ITAD media sanitizations standards promulgated by the United States Department of Defense long since superseded by the foregoing NIST standards and adopted the world over by ITAD professionals and their clients.

223. Chief among Morgan Stanley's deviations from the NIST standards was its failure to both properly encrypt customer PII on many of the IT Assets it decommissioned and sanitize that PII from those assets prior to giving them to Triple Crown.

224. Compounding these two failures was Morgan Stanley's extreme lack of diligence in supervising the ITAD process at several critical points during the decommissioning projects. This additional failure of due diligence led directly to Morgan Stanley's thorough lack of preparation to address and mitigate the harm caused when IT Assets containing unencrypted client PII found their way into the stream of commerce and the hands of criminals. By relying upon and failing to supervise unqualified vendor WeedHire/AnythingIT, Morgan Stanley recklessly, negligently, and otherwise violated the foregoing ITAD industry standards and, in so doing, breached its duties to Plaintiffs and Class Members.

3. Morgan Stanley Failed To Adhere to Its Own ITAD Policies Which Required Data Removal Before Asset Disposal.

225. Morgan Stanley's July 2, 2015 "Firmwide IT Data Decommissioning Procedure" ("the ITAD Procedure"), explained Morgan Stanley's responsibilities for assets for which Morgan Stanley removed data. The policy covered the "end of deployment of a device in its current use" and mandated that all content is removed before [IT Asset] disposal or redeployment." The ITAD Procedure made clear that IT Asset decommissioning was to be performed by authorized personnel or outsourced to a "Security Architecture (SecArch)-

approved vendor." The ITAD Procedure further provided that the procedures apply firmwide, and are "intended for all employees and third parties who need to decommission hardware that has been used to carry out Morgan Stanley business."

226. Morgan Stanley highlights these policies to clients and potential clients in a Cybersecurity letter. The letter begins, "Morgan Stanley's [] success depends on our reputation, which is built on integrity, excellence in service, honesty and fairness in all of our dealings. This reputation derives in part from our ability to maintain the confidentiality and security of information entrusted to us by our clients." In this letter, Morgan Stanley touts the effectiveness of its ITAD policy and third-party vendor controls. The letter states, that "[a] key control resident within these procedures is the cleansing of data from the asset prior to its removal from the Firm's environment."

227. The ITAD Procedure includes examples of compliant processes for IT Asset decommissioning for assets that remained operational and were to be disposed or re-deployed, and recommended that secure data removal required a "minimum 3x software wipe meeting DoD 5520.22M specifications." In addition, the ITAD Procedure required that the BIOS be reset if the asset was to be sent to a third party.

L. Securing PII and Preventing Data Security Incidents

228. Morgan Stanley's recklessness, carelessness, and negligence in safeguarding its customers' PII is exacerbated by the repeated warnings and alerts directed to protecting and securing electronics. And Morgan Stanley, specifically, had suffered breaches that involved stolen equipment containing customer PII only two years before this Data Security Incident.[39]

[39] Aruna Viswanatha, *Morgan Stanley Fined $1 Million for Client Data Breach*, The Wall Street Journal, June 8, 2016, available at: https://www.wsj.com/articles/morgan-stanley-fined-1-million-for-client-data-breach-1465415374 (last visited May 13, 2021).

Morgan Stanley has acknowledged the sensitive and confidential nature of the PII. To be sure, collecting, maintaining, and protecting PII is vital to many of Morgan Stanley's business purposes. Morgan Stanley 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 it may not disclose and must take reasonable steps to protect PII from improper release or disclosure. Despite the prevalence of public announcements of data breaches and data security compromises, and despite its own acknowledgments of data security compromises, and its duties to keep PII private and secure, Morgan Stanley failed to take appropriate steps to protect the PII of Plaintiffs and the proposed Class from being divulged.

229. The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority."[40] 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."[41]

230. The ramifications of Morgan Stanley'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 indefinitely.

[40] 17 C.F.R. § 248.201 (2013).

[41] *Id.*

M. Value of Personally Identifiable Information

231. The PII of consumers remains of high value to criminals, as evidenced by the prices they will pay for it on 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.[42] Experian reports that a stolen credit or debit card number can sell for $5 to $110 on the dark web.[43]

232. 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.[44]

233. What is more, it is difficult to change or cancel a stolen Social Security number. An individual cannot obtain a new Social Security number without significant paperwork and

---

[42] *Your personal data is for sale on the dark web. Here's how much it costs,* Digital Trends, Oct. 16, 2019, available at: https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/ (last accessed May 13, 2021).

[43] *Here's How Much Your Personal Information Is Selling for on the Dark Web*, Experian, Dec. 6, 2017, available at: https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/ (last accessed May 13, 2021).

[44] Social Security Administration, *Identity Theft and Your Social Security Number*, *available at:* https://www.ssa.gov/pubs/EN-05-10064.pdf (last visited May 13, 2021).

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 fraudulent activity to obtain a new number.

234. Even then, a new Social Security number may not be effective. According to Julie Ferguson of the Identity Theft Resource Center: "The credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[45]

235. Based on the foregoing, the information divulged in the Data Security Incident 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 divulged in the Data Security Incident is impossible to "close" and difficult, if not impossible, to change—such as Social Security numbers, passport numbers, names, dates of birth, addresses, asset holdings, and other financial information.

236. 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."[46]

237. 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.

---

[45] Bryan Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR (Feb. 9, 2015), available at: http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millionsworrying-about-identity-theft (last visited July 23, 2020).

[46] Time Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, IT World, (Feb. 6, 2015), *available at*: https://www.networkworld.com/article/2880366/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html (last visited July 23, 2020).

238. The fraudulent activity resulting from the Data Security Incidents may not come to light for years.

239. At all relevant times, Morgan Stanley 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 Morgan Stanley's data security system was compromised, including, specifically, the significant costs that would be imposed on Morgan Stanley's clients as a result of such an incident.

240. Plaintiffs and Class Members now face years of diligent 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.

241. Morgan Stanley was, or should have been, fully aware of the unique type and the significant volume of data on Morgan Stanley'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.

242. To date, Morgan Stanley has offered its customers only two years of credit monitoring service through a single credit bureau, Experian. This limited service is inadequate to protect Plaintiffs and Class Members from the threats they face for years to come, particularly in light of the PII at issue here.

243. The injuries to Plaintiffs and Class Members were directly and proximately caused by Morgan Stanley's failure to implement or maintain adequate data security measures for its current and former clients' PII.

N. Morgan Stanley Has Previously Exposed Customer Data

244. In early 2015, several media outlets reported that Morgan Stanley had discovered data related to about 900 of its client accounts on Pastebin, during a review of websites known to post such information.[47] Morgan Stanley determined that those accounts were among nearly 350,000 accounts that Galen Marsh, a Morgan Stanley financial adviser, had downloaded from Morgan Stanley databases. *Id*. The Wall Street Journal subsequently described the incident as "what some security experts are saying is likely the biggest data theft at a wealth-management firm."[48] The Wall Street Journal later reported that in fact data related to about 1,200 Morgan Stanley client accounts had appeared on Pastebin, and that the account information had "reappeared on several occasions" on other websites, including Twitter.[49]

245. In the course of a criminal proceeding against Mr. Marsh, the Department of Justice ("DOJ") disclosed that the Morgan Stanley software Mr. Marsh used to access the large volume of client data he downloaded was in fact supposed to limit his access to data related to his own clients.[50] He was nevertheless able to conduct thousands of searches of other Morgan Stanley clients' data over a period of more than three years, during which he uploaded what was

[47] Bloomberg News, *Financial Advisor Accused of Pilfering Data Working with Wirehouse*, Investment News (2015), *available at*: https://www.investmentnews.com/morgan-stanley-data-offered-on-internet-for-virtual-currency-60386 (last visited May 12, 2021).

[48] Justin Baer, *Puzzle Forms in Morgan Stanley Data Breach*, The Wall Street Journal, Jan. 7, 2015, *available at*: https://www.wsj.com/articles/puzzle-forms-in-morgan-stanley-data-breach-1420590326 (last visited May 12, 2021).

[49] Justin Baer, *U.S. Shifts Focus of Morgan Stanley Breach Probe*, The Wall Street Journal, Feb. 18, 2015, *available at:* https://www.wsj.com/articles/u-s-shifts-focus-of-morgan-stanley-breach-probe-1424305501 (last visited May 13, 2021).

[50] The Government's Sentencing Mem., at 2, *U.S. v. Marsh*, No. 15-cr-641 (D.D.C.), Dkt. No. 10 (filed Dec. 8, 2015).

in fact data from over 700,000 clients to his own personal server.[51] Morgan Stanley's investigation revealed that hackers gained access to Mr. Marsh's personal server over a period of several weeks in October 2014.[52]

246. The Securities and Exchange Commission ("SEC") subsequently instituted an investigation that resulted in the disclosure of additional information. According to the SEC, "[b]etween approximately December 15, 2014 and February 3, 2015, portions of this stolen data were posted to at least three Internet sites along with an offer to sell a larger quantity of stolen data in exchange for payment in speedcoins, a digital currency."[53]

247. Most significantly, the SEC found that Morgan Stanley: (1) "failed to ensure the reasonable design and proper operation of its policies and procedures in safeguarding confidential customer data"; (2) "failed to conduct any auditing or testing of the [deficient software modules] since their creation at least 10 years ago"; and (3) "did not monitor user activity in the [deficient software modules] to identify any unusual or suspicious patterns."[54]

248. The SEC determined that Morgan Stanley had "willfully violated Rule 30(a) of Regulation S-P (17 C.F.R. § 248.30(a)), which requires every broker-dealer and investment adviser registered with the Commission to adopt written policies and procedures that are reasonably designed to safeguard customer records and information."[55] Morgan Stanley was censured and required to a pay a penalty of $1,000,000.[56]

---

[51] *Id*. at 3.

[52] *Id*.

[53] Order, at 2, *In re Morgan Stanley Smith Barney, LLC*, Admin. Proc. File No. 3-17280 (June 8, 2016).

[54] *Id*. at 3-4.

[55] *Id*. at 6 (footnote omitted).

[56] *Id*.

O. The Data Security Incidents Have Caused Ongoing Harm to Plaintiffs

249. A breach of security, unauthorized access to current and former customer PII, and the resulting injury to Plaintiffs and Class Members was reasonably foreseeable, particularly in light of the acknowledged inadequacy of Defendant's ITAD practices.

250. Plaintiffs and Class Members were the foreseeable and probable victims of Morgan Stanley's inadequate ITAD security practices and procedures. Indeed, Morgan Stanley knew or should have known of the inherent risks in collecting and storing the PII of Plaintiffs and Class members, the critical importance of providing adequate security over that PII, and the necessity for encrypting PII stored on Morgan Stanley's IT Assets.

251. Morgan Stanley's own conduct created a foreseeable risk of harm to Plaintiffs and Class Members. Morgan Stanley's misconduct included, but was not limited to, its failure to take the steps and opportunities to prevent both the Data Security Incidents.

252. Morgan Stanley's reckless misconduct also included its decisions to not comply with prevailing ITAD industry standards for the destruction of IT Assets and the sanitization of Plaintiffs and Class Members PII, including its failure to employ widely used encryption techniques prior to transferring IT Assets to Triple Crown and WeedHire/AnythingIT.

253. The ramifications of Morgan Stanley's failure to keep Plaintiffs' and Class members' PII secure are substantial.

254. Consumer victims of data breaches are much more likely to become victims of identity fraud. This conclusion is based on an analysis of four years of data that correlated each year's data breach victims with those who also reported being victims of identity fraud.[57]

[57] 2014 LexisNexis True Cost of Fraud Study, https://www.lexisnexis.com/risk/downloads/assets/true-cost-fraud-2014.pdf.

255. PII is a valuable commodity to identity thieves once the information has been divulged or compromised. As the FTC recognizes, once identity thieves have personal information, "they can drain your bank account, run up your credit cards, open new utility accounts, or get medical treatment on your health insurance."[58]

256. Identity thieves can use personal information, such as that of Plaintiffs and Class Members, which Morgan Stanley failed to keep secure, to perpetrate a variety of crimes that harm victims. For instance, identity thieves may commit various types of government fraud such as: immigration fraud; obtaining a driver's license or identification card in the victim's name but with another's picture; using the victim's information to obtain government benefits; or filing a fraudulent tax return using the victim's information to obtain a fraudulent refund.

257. Javelin Strategy and Research reports that identity thieves stole $112 billion from 2010 to 2016—which has increased since 2016 with the proliferation of data breaches.[59]

258. Reimbursing a consumer for a financial loss due to fraud does not make that individual whole again. On the contrary, identity theft victims must spend numerous hours and their own money repairing the impact to their credit. After conducting a study, the Department of Justice's Bureau of Justice Statistics found that identity theft victims "reported spending an average of about 7 hours clearing up the issues" and resolving the consequences of fraud in 2014.[60]

---

[58] Federal Trade Commission, *Warning Signs of Identity Theft, available at:* https://www.consumer.ftc.gov/articles/0271-warning-signs-identity-theft (last visited May 13, 2021).

[59] https://www.javelinstrategy.com/coverage-area/2016-identity-fraud-fraud-hits-inflection-point

[60] *Victims of Identity Theft*, 2014 (Sept. 2015) *available at:* http://www.bjs.gov/content/pub/pdf/vit14.pdf.

259. An independent financial services industry research study conducted for BillGuard—a private entity that automates the consumer task of finding unauthorized transactions that might otherwise go undetected—calculated the average per-consumer cost of all unauthorized transactions at roughly $215 per cardholder incurring these charges,[61] some portion of which could go undetected and thus must be paid entirely out-of-pocket by consumer victims of account or identity misuse. This figure is based on misuse of cardholder information, which is less valuable than the PII at issue here—including full names, dates of birth, Social Security numbers, and other information which can easily be used to open credit accounts and other financial accounts to perpetrate further fraud, increasing the amount of average damages.

260. The litany of complaints regarding identify theft and similar incidents to Morgan Stanley from victimized Class Members is indicative of the consequences of the Data Security Incidents. *See* ¶¶ 23, 24, 261-354.

1. Plaintiffs John and Midori Nelson's Experience

261. On November 11, 2000, Ms. Nelson opened her IRA account at Morgan Stanley with the assistance of her brother, who was then employed at Morgan Stanley as a financial analyst. When opening her account, Ms. Nelson listed her husband, John Nelson, as the sole beneficiary of all proceeds of her IRA account. Morgan Stanley asked Ms. Nelson to supply her and Mr. Nelson's PII, including but not limited to their names, address, and Social Security numbers. Ms. Nelson closed her account on July 14, 2003 after her brother stopped working for Morgan Stanley.

[61] Hadley Malcom, *Consumers rack up $14.3 billion in gray charges*, research study commissioned for Billguard by Aite Research, USA Today (July 25, 2013), *available at:* https://www.usatoday.com/story/money/personalfinance/2013/07/25/consumers-unwanted-charges-in-billions/2568645/.

262. Mr. and Ms. Nelson received the Notice of Data Breach, dated July 10, 2020, on or about that date. It was addressed to "John C. Nelson & Midori T. Nelson JT Ten."

263. In or about June 2019, unknown third parties used Ms. Nelson's credit card to make unauthorized purchases. Her credit card company confirmed the fraud and reimbursed her. Later in 2019, unknown third parties used the same credit card account to make additional unauthorized purchases. The credit card company again confirmed the fraud and reimbursed the account. Both times, the Nelsons were unable to use the credit card for approximately one week before each card was replaced by mail.

264. As a result of the Notice of Data Breach and the fraudulent credit card charges, Mr. and Ms. Nelson have spent time dealing with the consequences of the Data Security Incidents, which includes time spent verifying the legitimacy of the Notice of Data Breach, reviewing their financial accounts statements, visiting their bank and contacting their credit union and credit card companies about possible financial consequences, and routinely monitoring their credit for suspicious activity on credit bureau websites. Moreover, over the past few years, the Nelsons have repeatedly received phishing telephone calls. The calls became so frequent they purchased an electronic device designed to block these messages. This time and expense can never be recovered, and particularly for Ms. Nelson, who suffers from chronic and often debilitating illness, it is time spent suffering through tasks that needlessly tax her physically, mentally, and emotionally.

265. Mr. and Ms. Nelson are very careful about sharing their PII, and have never knowingly transmitted unencrypted PII over the internet or any other unsecured source.

266. Mr. and Ms. Nelson suffered actual injury and damages in paying annual fees to Defendant for facilitating Ms. Nelson's trading account before the Data Security Incidents,

expenditures that they would not have incurred had Defendant disclosed that it lacked data security practices adequate to safeguard customers' PII.

267. Mr. and Ms. Nelson suffered actual injury in the form of damages to and diminution in the value of their PII—a form of intangible property—that they both entrusted to Morgan Stanley for the purpose of facilitating Ms. Nelson's retirement account, which was divulged in the Data Security Incidents.

268. Mr. and Ms. Nelson suffered lost time, annoyance, interference, and inconvenience as a result of the Data Security Incidents and have anxiety and increased concerns for the loss of their privacy.

269. Mr. and Ms. Nelson have suffered and will continue to suffer imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from their PII, especially their Social Security numbers, being placed in the hands of criminals and other unauthorized third parties.

270. Mr. and Ms. Nelson have a continuing interest in ensuring that their PII that remains stored in Morgan Stanley's computer systems is sufficiently protected and safeguarded from future data security incidents.

2. Plaintiff Sylvia Tillman's Experience

271. In the early or mid-1990s, Plaintiff Sylvia Tillman signed up for a California Uniform Transfers to Minors Act ("UTMA/CA") account for her minor daughter through Morgan Stanley in California. A UTMA/CA account allows an appointed custodian to manage the minor's account until the latter turns 18. Ms. Tillman supplied Morgan Stanley with her and her daughters' PII, including but not limited to their address and Social Security numbers. Ms. Tillman closed the UTMA/CA account in or about 2000. At the time of the Data Security Incidents, Ms. Tillman was not a Morgan Stanley client.

272. Ms. Tillman received the Notice of Data Breach, dated July 11, 2020, on or about that date. It was addressed to "Sylvia Tillman cust[odian] for [her minor daughter] UTMA/CA."

273. As a result of the Data Breach notice, Ms. Tillman spent time dealing with the consequences of the Data Security Incidents, which includes time spent verifying the legitimacy of the Notice of Data Breach, communicating with Morgan Stanley representatives on the toll-free number supplied in the notice, exploring credit monitoring and identity theft insurance options, and self-monitoring her accounts. This time has been lost and cannot be recaptured.

274. Ms. Tillman is very careful about sharing her PII, and has never knowingly transmitted unencrypted PII over the internet or any other unsecured source.

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

276. Ms. Tillman suffered actual injury and damages in paying money to Morgan Stanley for facilitating the UTMA/CA account before the Data Security Incidents, expenditures which she would not have made had Morgan Stanley disclosed that it lacked data security practices adequate to safeguard customers' PII.

277. Ms. Tillman suffered actual injury in the form of damages to and diminution in the value of her PII—a form of intangible property—that Ms. Tillman entrusted to Morgan Stanley for the purpose of facilitating the UTMA/CA account, which was divulged as a result of the Data Security Incidents.

278. Ms. Tillman suffered lost time, annoyance, interference, and inconvenience as a result of the Data Security Incidents and has anxiety and increased concerns for the loss of her privacy.

279. Ms. Tillman has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from her PII, especially her and her daughters' Social Security numbers, being placed in the hands of unauthorized third-parties and possibly criminals.

280. Ms. Tillman has a continuing interest in ensuring that her PII, which, upon information and belief, remains stored in Morgan Stanley's possession, is protected and safeguarded from future breaches.

3. Plaintiff Mark Blythe's Experiences

281. In or about 2012, Plaintiff Mark Blythe signed up for a stock account and an annuity account through Morgan Stanley. Mr. Blythe supplied Morgan Stanley with PII, including but not limited to his name, address, and Social Security number. Both accounts were closed on October 3, 2017.

282. Mr. Blythe received the Notice of Data Breach, dated July 10, 2020, on or about July 28, 2020.

283. In or about July 2020, Mr. Blythe suffered a string of identity thefts involving the Navy Federal Credit Union in Virginia and misuse of his personal information through no fault of his own. On or about July 6, 2020, an unauthorized third party opened a checking account with a credit union in Mr. Blythe's name. On or about July 7, 2020, an unauthorized third party applied for a Small Business Administration ("SBA") loan with the same credit union in Mr. Blythe's name. On or about July 15, 2020, an unauthorized third party opened a savings account in Mr. Blythe's name. On or about July 17, 2020, Mr. Blythe learned of the identity theft because

of the credit union directly reporting to Experian, with whom Mr. Blythe had purchased credit monitoring. Specifically, the credit union pulled Mr. Blythe's credit during the process of making an SBA loan to an unauthorized third party.

284. As a result of the Data Breach notice and identity theft, Mr. Blythe spent time dealing with the consequences of the Data Security Incidents, which includes verifying the legitimacy of the Notice of Data Breach, communicating with credit reporting agencies, and investigating and attempting to stop fraudulent uses of his divulged PII by unauthorized third parties, which included filing a police report with the Flagler Beach Police Department and notifying a credit union multiple times of fraudulent uses of Mr. Blythe's PII at that credit union. Additionally, Mr. Blythe now monitors his credit regularly using Experian professional software and, when these issues arose, he immediately contacted Experian, the credit union, and other authorities. Having learned of the identify theft, Mr. Blythe and his wife both went into credit lock due to the fraudulent activity. Mr. Blythe thereafter maintained his "Professional Credit Monitoring Profile" with Experian. This time has been lost forever and cannot be recaptured.

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

286. Mr. Blythe stores any and all documents 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, he diligently chooses unique usernames and passwords for his various online accounts.

287. Mr. Blythe suffered actual injury and damages in paying money to Morgan Stanley for facilitating his stock account and an annuity account, expenditures which he would

not have made had Morgan Stanley disclosed that it lacked data security practices adequate to safeguard customers' PII.

288. Mr. Blythe suffered actual injury in the form of damages to and diminution in the value of his PII—a form of intangible property—that Mr. Blythe entrusted to Morgan Stanley for the purpose of facilitating his stock account and annuity account, which was divulged as a result of the Data Security Incidents.

289. Mr. Blythe suffered lost time, annoyance, interference, and inconvenience as a result of the Data Security Incidents and has anxiety and increased concerns for the loss of his privacy.

290. Mr. Blythe has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from his PII being placed in the hands of unauthorized third parties and possibly criminals.

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

4. Plaintiff Vivian Yates' Experiences

292. Vivian Yates established a 529 college savings plan account with Morgan Stanley in or about 2015. Ms. Yates supplied Morgan Stanley with her PII, including but not limited to her name, address, Social Security number, and other financial information.

293. Ms. Yates received Morgan Stanley's Notice of Data Breach, dated July 10, 2020, on or about that date.

294. As a result of the Data Breach notice, Ms. Yates spent time dealing with the consequences of the Data Security Incidents, which includes time spent verifying the legitimacy of the Notice of Data Breach, communicating with Morgan Stanley representatives on the toll-

free number supplied in the notice, exploring credit monitoring and identity theft insurance options, and self-monitoring her accounts. This time has been lost forever and cannot be recaptured.

295. Ms. Yates is very careful about sharing her PII and has never knowingly transmitted unencrypted PII over the internet or any other unsecured source.

296. Ms. Yates stores any and all documents containing her PII in a safe and secure digital location and destroys any documents she receives in the mail that contain any of her PII, or that may contain any information that could otherwise be used to compromise her credit card accounts and identities. Moreover, she diligently chooses unique usernames and passwords for her various online accounts.

297. Ms. Yates suffered actual injury and damages in paying money to Morgan Stanley for facilitating her accounts before the Data Security Incidents, expenditures which she would not have made had Morgan Stanley disclosed that it lacked data security practices adequate to safeguard customers' PII.

298. Ms. Yates suffered actual injury in the form of damages to and diminution in the value of her PII—a form of intangible property—that she entrusted to Morgan Stanley for the purpose of facilitating her accounts, which was divulged as a result of the Data Security Incident.

299. Ms. Yates suffered lost time, annoyance, interference, and inconvenience as a result of the Data Security Incidents and has anxiety and increased concerns for the loss of her privacy.

300. Ms. Yates has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from her lost PII,

especially her Social Security number being placed in the hands of unauthorized third parties and possibly criminals.

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

5. Plaintiffs Richard and Cheryl Gamen's Experiences

302. In or about 1989, Plaintiffs Richard Gamen and his wife, Cheryl Gamen, signed up for a brokerage account through Morgan Stanley's office in Chicago, Illinois. The Gamens supplied Morgan Stanley with their PII, including but not limited to their names, address, and Social Security numbers. The brokerage account was terminated in or about 2010.

303. Mrs. Gamen, in the early 1990's, also rolled over her 401(k) individual retirement account to a Morgan Stanley IRA. That account was terminated in or about 2001.

304. Mr. and Mrs. Gamen received a joint Notice of Data Breach, dated July 11, 2020, on or about that date, for the brokerage account. Ms. Gamen received another Notice of Data Breach, dated July 11, 2020, on or about July 26, 2020, for her IRA account.

305. In or about June 2020, Mr. Gamen began receiving an increasing number of scam telephone calls on a regular basis. The calls claim his Social Security number is "locked" and that he will be arrested unless he interacts with the caller. Mr. Gamen has also received an increasing number of emails from fraudsters claiming a foreign person has died and the fraudster is reaching out to share money.

306. As a result of the Data Breach notices and the scam calls and emails, Mr. and Mrs. Gamen spent time dealing with the consequences of the Data Security Incidents, which includes time spent verifying the legitimacy of the Notice of Data Breach, communicating with Morgan Stanley representatives on the toll-free number supplied in the notice, exploring credit

monitoring and identity theft insurance options, and self-monitoring their accounts. Mr. and Mrs. Gamen also filed an online complaint with the Federal Trade Commission regarding the Data Security Incidents. This time has been lost forever and cannot be recaptured.

307. Mr. and Ms. Gamen are very careful about sharing their PII, and have never knowingly transmitted unencrypted PII over the internet or any other unsecured source.

308. Mr. and Mrs. Gamen store any and all documents containing their PII in a safe and secure digital location, and destroy any documents they receive in the mail that contain any of their PII, or that may contain any information that could otherwise be used to compromise their credit card accounts and identities. Moreover, they diligently choose unique usernames and passwords for their various online accounts.

309. Mr. and Mrs. Gamen suffered actual injury and damages in paying money to Morgan Stanley for facilitating their accounts before the Data Security Incidents, expenditures which they would not have made had Morgan Stanley disclosed that it lacked data security practices adequate to safeguard customers' PII.

310. Mr. and Mrs. Gamen suffered actual injury in the form of damages to and diminution in the value of their PII—a form of intangible property—that Mr. and Mrs. Gamen entrusted to Morgan Stanley for the purpose of facilitating their accounts, which was divulged as a result of the Data Security Incidents.

311. Mr. and Mrs. Gamen suffered lost time, annoyance, interference, and inconvenience as a result of the Data Security Incidents and have anxiety and increased concerns for the loss of their privacy.

312. Mr. and Mrs. Gamen have suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from their lost PII,

especially their Social Security numbers being placed in the hands of unauthorized third parties and possibly criminals.

313. Mr. and Mrs. Gamen have a continuing interest in ensuring that their PII, which, upon information and belief, remains backed up in Morgan Stanley's possession, is protected and safeguarded from future breaches.

6. Plaintiff Amresh Jaijee's Experience

314. In or about 2012, Plaintiff Amresh Jaijee rolled over her 401(k) individual retirement account ("IRA") to a Morgan Stanley IRA at one of Morgan Stanley's offices in New York City. Ms. Jaijee supplied Morgan Stanley with her PII, including but not limited to her name, address, Social Security number, personal identification, checking account number and other financial information. She listed beneficiaries to her account and included their contact information. Ms. Jaijee's Morgan Stanley account is still active.

315. Ms. Jaijee received the Notice of Data Breach, dated July 10, 2020, on or about that date. It specifically states that in addition to her Social Security number, information about "any linked bank accounts" was breached as well.

316. In or around the end of June 2020, Ms. Jaijee received a telephone call from an individual claiming to represent an insurance company. This individual knew her Social Security number and attempted to have her verify it and her bank routing number. Ms. Jaijee later called the insurance company and confirmed her suspicions that the earlier call was a scam.

317. Since in or about June 2020, Ms. Jaijee has received an increasing number of scam telephone calls, some displaying "JP Morgan/Chase" on her Caller ID, but the corresponding messages are in Chinese.

318. As a result of the Data Breach notice and the scam telephone calls, Ms. Jaijee spent time dealing with the consequences of the Data Security Incidents, which includes time

spent verifying the legitimacy of the Notice of Data Breach and the insurance company call, communicating with representatives of her bank that is linked to the Morgan Stanley IRA, alerting her credit card companies and the three credit bureaus about the Data Security Incidents, routinely checking her credit monitoring (for which she continues to pay approximately $18 per month), exploring further credit monitoring and identity theft insurance options, and self-monitoring her accounts. This time has been lost forever and cannot be recaptured.

319. Ms. Jaijee attempted to register for the Experian credit monitoring offered by Morgan Stanley but was unsuccessful. She contacted Experian to assist her in signing up, but the technician told her that "passwords were being updated" and that someone from Experian would contact her to assist. To date, Ms. Jaijee is waiting to hear back from Experian. She is still unable to register with Experian despite having the Notice of Data Breach addressed to her.

320. Ms. Jaijee stores any and all documents containing her PII in a safe and secure digital location and destroys any documents she receives in the mail that contain her Social Security number or any other vital PII.

321. Ms. Jaijee suffered actual injury and damages in paying annual fees to Morgan Stanley for facilitating her 401(k) IRA account before the Data Security Incidents, expenditures which she would not have made had Morgan Stanley disclosed that it lacked data security practices adequate to safeguard customers' PII.

322. Ms. Jaijee suffered actual injury in the form of damages to and diminution in the value of her PII—a form of intangible property—that Ms. Jaijee entrusted to Morgan Stanley for the purpose of facilitating her 401(k) IRA account, which was divulged as a result of the Data Security Incidents.

323. Ms. Jaijee suffered lost time, annoyance, interference, and inconvenience as a result of the Data Security Incidents. Ms. Jaijee was recently telephoned by an unidentified party who had her Social Security number and asked her to verify it..

324. Ms. Jaijee has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from her PII, especially her Social Security number being placed in the hands of unauthorized third-parties and possibly criminals.

325. Ms. Jaijee has a continuing interest in ensuring that her PII, which, upon information and belief, remains stored in Morgan Stanley's possession, is protected and safeguarded from future breaches.

7. Plaintiff Richard Mausner's Experience

326. Plaintiff Richard Mausner signed up for an account at Morgan Stanley in New Jersey. Mr. Mausner supplied Morgan Stanley with his PII, including but not limited to his name, address, and Social Security number in connection with the opening of this account. Mr. Mausner closed the account no later than 2010.

327. Mr. Mausner received the Notice of Data Breach, dated July 11, 2020, on or about that date.

328. As a result of the Data Breach notice, Mr. Mausner spent time dealing with the consequences of the Data Security Incidents, which includes time spent verifying the legitimacy of the Notice of Data Breach, placing a credit freeze, contacting his bank, exploring credit monitoring and identity theft insurance options, and self-monitoring his accounts. This time has been lost forever and cannot be recaptured.

329. Mr. Mausner stores documents 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, he diligently chooses unique usernames and passwords for his online accounts.

330. Mr. Mausner suffered actual injury and damages in paying money to Morgan Stanley for facilitating his account before the Data Security Incidents, expenditures which he would not have made had Defendant disclosed that it lacked data security practices adequate to safeguard customers' PII.

331. Mr. Mausner suffered actual injury in the form of damages to and diminution in the value of his PII—a form of intangible property—that Mr. Mausner entrusted to Defendant for the purpose of facilitating his account, which was divulged as a result of the Data Security Incidents.

332. Mr. Mausner suffered lost time, annoyance, interference, and inconvenience as a result of the Data Security Incidents and has anxiety and increased concerns for the loss of his privacy.

333. Mr. Mausner has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from his lost PII, especially his Social Security number being placed in the hands of unauthorized third parties and possibly criminals.

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

8. Plaintiff Desiree Shapouri's Experience

335. Plaintiff Desiree Shapouri signed up for an account with Morgan Stanley in New York in or about 2007. Ms. Shapouri was asked to and did supply Morgan Stanley with her PII,

including but not limited to her address and Social Security number in connection with the opening of this account. Ms. Shapouri closed her account in or about 2011.

336. Ms. Shapouri received the Notice of Data Breach, dated July 11, 2020, on or about that date.

337. From September 3, 2019 through September 18, 2019, Ms. Shapouri experienced twelve separate unauthorized charges on her credit card.

338. As a result of the Data Breach notice, Ms. Shapouri spent time dealing with the consequences of the Data Security Incidents, which includes exploring credit monitoring and identity theft insurance options, and self-monitoring her accounts. She also initiated a credit freeze with TransUnion and Equifax, as well as purchased identify theft protection with Identity Guard. This time has been lost forever and cannot be recaptured.

339. Ms. Shapouri is very careful about sharing her PII, and stores documents containing her PII in a safe and secure digital location and destroys documents she receives in the mail that may contain her PII, or that may contain any information that could otherwise be used to compromise her credit card accounts and identity. Moreover, she diligently chooses unique usernames and passwords for her various online accounts.

340. Ms. Shapouri suffered actual injury and damages in paying money to Morgan Stanley for facilitating her stock account and an annuity account; expenditures which she would not have made had Morgan Stanley disclosed that it lacked data security practices adequate to safeguard customers' PII.

341. Ms. Shapouri suffered actual injury in the form of damages to and diminution in the value of her PII—a form of intangible property—that Ms. Shapouri entrusted to Defendant

for the purpose of facilitating her account, which was divulged as a result of the Data Security Incidents.

342. Ms. Shapouri suffered lost time, annoyance, interference, and inconvenience as a result of the Data Security Incidents and has anxiety and increased concerns for the loss of her privacy.

343. Ms. Shapouri has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from her PII, including her Social Security number, being placed in the hands of unauthorized third parties and possibly criminals.

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

9. Plaintiff Howard Katz's Experience

345. In or about the end of 2012, Plaintiff Howard Katz signed up for a trading account with Morgan Stanley via telephone. When he opened his account, Morgan Stanley asked Mr. Katz to supply his PII, including but not limited to his name, address, and Social Security number. Mr. Katz closed the account in or about 2016.

346. Mr. Katz received the Notice of Data Breach, dated July 10, 2020, on or about that date.

347. As a result of the Data Breach notice, Mr. Katz spent time dealing with the consequences of the Data Security Incidents, which includes time spent verifying the legitimacy of the Notice of Data Breach, checking his credit monitoring (which he continues to pay approximately $125 per year), exploring further credit monitoring and identity theft insurance

options, visiting his bank, and self-monitoring his accounts. This time has been lost forever and cannot be recaptured.

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

349. Mr. Katz 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. Katz diligently chooses unique usernames and passwords for his various online accounts.

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

351. Mr. Katz suffered actual injury in the form of damages to and diminution in the value of his PII – a form of intangible property – that Mr. Katz entrusted to Morgan Stanley for the purpose of facilitating his trading account, which was divulged as a result of the Data Security Incidents.

352. Mr. Katz suffered lost time, annoyance, interference, and inconvenience as a result of the Data Security Incidents and has anxiety and increased concerns for the loss of his privacy.

353. Mr. Katz has suffered and will continue to suffer imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from his

PII, especially his Social Security number, being placed in the hands of criminals and other unauthorized third parties.

354. Mr. Katz has a continuing interest in ensuring that his PII that remains stored in Morgan Stanley's computer systems and is sufficiently protected and safeguarded from future data breaches.

CLASS ALLEGATIONS

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

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

> All individuals with existing or closed Morgan Stanley accounts established in the United States whose PII was divulged in the Data Security Incidents.

357. Excluded from the Class are the following individuals and/or entities: Morgan Stanley and Morgan Stanley's parents, subsidiaries, affiliates, officers and directors, current or former employees, and any entity in which Morgan Stanley 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.

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

359. Numerosity, Fed R. Civ. P. 23(a)(1): The Class is so numerous that joinder of all members is impracticable. Morgan Stanley has identified millions of customers whose PII may

have been improperly divulged in the Data Security Incidents, and the Class is apparently identifiable within Morgan Stanley's records.

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

a. Whether and to what extent Morgan Stanley had a duty to protect the PII of Plaintiffs and Class Members, including by nature of the fiduciary relationship between Morgan Stanley and Plaintiffs and Class Members;

b. Whether Morgan Stanley had respective duties not to divulge the PII of Plaintiffs and Class Members to unauthorized third parties;

c. Whether Morgan Stanley had respective duties not to use the PII of Plaintiffs and Class Members for purposes beyond Plaintiffs' and Class Members' consent;

d. Whether Morgan Stanley breached these legal duties to Plaintiffs and Class Members to exercise due care in collecting, storing, using, and safeguarding their PII;

e. When Morgan Stanley actually learned of each of the Data Security Incidents;

f. Whether Morgan Stanley adequately, promptly, and accurately informed Plaintiffs and Class Members that their PII had been divulged;

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

h. Whether Morgan Stanley failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information divulged in the Data Security Incidents;

i. Whether Morgan Stanley adequately addressed and fixed the vulnerabilities which permitted the Data Security Incidents to occur;

j. Whether Morgan Stanley failed to comply with its own policies and all applicable laws, regulations, and industry standards relating to data security;

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

l. Whether Plaintiffs and Class Members are entitled to actual damages, nominal damages, statutory damages, and/or punitive damages as a result of Morgan Stanley's wrongful conduct;

m. Whether Plaintiffs and Class Members are entitled to restitution as a result of Morgan Stanley's wrongful conduct;

n. Whether Plaintiffs and Class Members are entitled to injunctive relief to redress the imminent and currently ongoing harm faced as a result of the Data Security Incidents; and

o. Whether Morgan Stanley violated the New York Consumer Law for Deceptive Acts and Practices New York Gen. Bus. Law § 349.

361. Typicality, Fed. R. Civ. P. 23(a)(3): Plaintiffs' claims are typical of those of other Class Members because all had their PII divulged as a result of the Data Security Incidents, due to Morgan Stanley's misfeasance.

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

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

364. 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 Morgan Stanley. 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.

365. The nature of this action and the nature of laws available to Plaintiffs and Class Members make the use of the class action device a particularly efficient and appropriate procedure to afford relief to Plaintiffs and Class Members for the wrongs alleged because Morgan Stanley would necessarily gain an unconscionable advantage since they would be able to exploit and overwhelm the limited resources of each individual Class Member with superior financial and legal resources; the costs of individual suits could unreasonably consume the amounts that would be recovered; proof of a common course of conduct to which Plaintiffs were exposed is representative of that experienced by the Class and will establish the right of each Class Member to recover on the cause of action alleged; and individual actions would create a risk of inconsistent results and would be unnecessary and duplicative of this litigation.

366. The litigation of the claims brought herein is manageable. Morgan Stanley'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.

367. Adequate notice can be given to Class Members directly using information maintained in Morgan Stanley's records.

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

369. Further, Morgan Stanley 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.

370. 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 those enumerated in Paragraph 360.

NEW YORK LAW APPLIES TO THE CLASS

371. The laws of New York should govern Plaintiffs' claims and, therefore, the claims of the Class that Plaintiffs seek to represent.

372. Morgan Stanley is headquartered at 1585 Broadway, New York, New York, with its principal place of business in New York, New York. Upon information and belief, the headquarters is the "nerve center" of Morgan Stanley's business activities—the place where its executive-level and similarly-responsible officers, directors, and other high-level employees direct, control, and coordinate the corporation's activities, including its data security functions and major policy and legal decisions.

373. New York has a significant interest in regulating the conduct of businesses operating within its borders. New York, which seeks to protect the rights and interests of residents and citizens of the United States against financial companies headquartered and doing business in New York, has a greater interest in the claims of Plaintiffs and members of the Class than any other state and is most intimately concerned with the claims and outcome of this litigation.

374. Upon information and belief, all contracts that Plaintiffs and Class Members reviewed and executed were created by Morgan Stanley in New York.

375. Upon information and belief, all monies that Plaintiffs and Class Members paid to Morgan Stanley for its products were ultimately delivered to Morgan Stanley in New York.

376. Upon information and belief, Morgan Stanley's clearinghouse practices and decisions related thereto—including the disposal of servers and computer equipment at issue in this Data Security Incidents—were made from and in New York.

377. Upon information and belief, Morgan Stanley's decisions regarding the Decommissioning, as well as the decisions regarding its response to the Data Security Incidents, were made in and emanated from New York.

378. Application of New York law to Plaintiffs' and Class Members' claims would be neither arbitrary nor fundamentally unfair because New York has a significant interest in the claims of Plaintiffs and members of the Class.

379. Under choice of law principles applicable to this litigation, the common law of New York would apply to the common law claims, as well as the New York law claims, of all class members because of New York's significant interest in regulating the conduct of businesses—Morgan Stanley included—operating within its borders. Thus, New York's consumer protection laws may be applied to non-resident consumers across the United States.

380. Alternatively, the law governing Plaintiffs' common law claims alleged herein on behalf of the Class does not differ materially across the states in which Class Members reside or create predominating individual issues of law sufficient to impede the certification of the Class.

CAUSES OF ACTION

COUNT I
Negligence
(On Behalf of Plaintiffs and the Class)

381. Plaintiffs re-allege and incorporate by reference paragraphs 1-354 and 371-380 as though fully alleged herein.

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

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

384. Morgan Stanley has full knowledge of the sensitivity of the PII and the types of harm that Plaintiffs and Class Members could and would suffer if the PII were wrongfully disclosed.

385. Morgan Stanley 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 Plaintiffs and Class Members, even if the harm occurred through the criminal acts of a third party.

386. Morgan Stanley had a duty to exercise reasonable care in safeguarding, securing, and protecting such information from being compromised, lost, stolen, misused, and/or divulged to unauthorized parties. This duty includes, among other things, designing, maintaining, and testing Morgan Stanley's security protocols for its computer systems, data security practices, and disposal practices to ensure that Plaintiffs' and Class Members' information in Morgan Stanley's possession was adequately secured and protected.

387. Morgan Stanley also had a duty to exercise appropriate clearinghouse practices to remove former customers' PII it was no longer required to retain pursuant to regulations.

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

389. Morgan Stanley's duty to use reasonable security measures arose as a result of the special relationship that existed between Defendant and Plaintiffs and Class Members. That special relationship arose because Plaintiffs and Class Members entrusted Morgan Stanley with their confidential PII, a necessary part of the process of establishing an account with the company.

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

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

392. Plaintiffs and Class Members were the foreseeable and probable victims of any inadequate security practices and procedures. Morgan Stanley knew or should have known of the inherent risks in collecting and storing the PII of Plaintiffs and Class Members, the critical importance of providing adequate security of that PII, the necessity for encrypting PII stored on Morgan Stanley's systems, and the importance of ensuring that appropriate disposal practices were employed for the decommissioning of IT Assets containing PII.

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

394. Plaintiffs and the Class Members had no ability to protect their PII that was in, and likely remains in, Morgan Stanley's possession.

395. Morgan Stanley was in a position to protect against the harm suffered by Plaintiffs and Class Members as a result of the Data Security Incidents.

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

397. Morgan Stanley had a duty to employ proper procedures to prevent the unauthorized dissemination of the PII of Plaintiffs and Class Members.

398. Morgan Stanley has admitted that the PII of Plaintiffs and Class Members was wrongfully lost and disclosed to unauthorized third persons as a result of the Data Security Incidents.

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

400. Morgan Stanley improperly and inadequately safeguarded the PII of Plaintiffs and Class Members in deviation of standard industry rules, regulations, and practices at the time of the Data Security Incidents.

401. Morgan Stanley improperly and inadequately disposed of IT Assets containing the PII of Plaintiffs and Class Members in deviation of standard industry rules, regulations, and practices as the time of the Data Security Incidents.

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

403. Morgan Stanley breached its duty to exercise appropriate clearinghouse practices by failing to remove former customers' PII it was no longer required to retain pursuant to regulations.

404. Morgan Stanley, through its actions and/or omissions, unlawfully breached its duty to adequately and timely disclose to Plaintiffs and Class Members the existence and scope of the Data Security Incidents.

405. But for Morgan Stanley's wrongful and negligent breach of duties owed to Plaintiffs and Class Members, the PII of Plaintiffs and Class Members would not have been divulged.

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

407. Additionally, Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or

practice by businesses, such as Morgan Stanley, of failing to use reasonable measures to protect PII. The FTC publications and orders described above also form part of the basis of Morgan Stanley's duty in this regard.

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

409. Morgan Stanley's violation of Section 5 of the FTC Act constitutes negligence *per se*.

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

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

412. As a direct and proximate result of Morgan Stanley's negligence and negligence *per se*, Plaintiffs and Class Members have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the inherent value of their PII; (iii) the divulgence, 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 Security Incidents, 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 Morgan Stanley's possession and is subject to further unauthorized disclosures so long as Morgan Stanley fails to undertake appropriate and adequate measures to protect the PII of 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 divulged as a result of the Data Security Incidents for the remainder of the lives of Plaintiffs and Class Members; (ix) the diminished value of Morgan Stanley's goods and services they received; and (x) nominal damages.

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

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

COUNT II
Gross Negligence
(On Behalf of Plaintiffs and the Class)

415. Plaintiffs re-allege and incorporate by reference paragraphs 1-354 and 371-380 as though fully alleged herein.

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

417. Morgan Stanley's networks, systems, protocols, policies, procedures, and practices, as described above, were not adequately designed, implemented, maintained, monitored, and tested to ensure that Plaintiffs' and Class Members' PII was secured from release, disclosure, and publication.

418. Morgan Stanley's networks, systems, protocols, policies, procedures, and practices, as described above, were not reasonable given the sensitivity of the Plaintiffs' and Class Members' private data and the known vulnerabilities of Morgan Stanley's protocols, policies, procedures, and practices.

419. Upon learning of the 2016 Data Security Incident, Morgan Stanley should have immediately disclosed that event to Plaintiffs and Class Members, credit reporting agencies, the Internal Revenue Service, regulators, financial institutions, and all other third parties with a right to know and the ability to mitigate harm to Plaintiffs and Class Members as a result of that event.

420. At all times material hereto, Morgan Stanley knew and intentionally and/or recklessly disregarded the fact that its protocols, policies, procedures, and practices, as described above, were not adequately designed, implemented, maintained, monitored, and tested to ensure that Plaintiffs' and Class Members' PII was secured from release, disclosure, and publication. Morgan Stanley ignored these inadequacies and was indifferent to the risk of release, disclosure, and publication it had created.

421. At all times material hereto, Morgan Stanley attempted to misrepresent and did misrepresent facts concerning the security of its clients' PII.

422. Morgan Stanley's misrepresentations included knowingly withholding material information from the financial community and the public, including Plaintiffs and Class Members, concerning the security of its clients' PII.

423. Morgan Stanley's misconduct was aggravated by the type of grossly negligent disregard for the interests of Plaintiffs and Class Members for which the law would allow, and for which Plaintiffs will seek at the appropriate time, the imposition of punitive damages, in that Morgan Stanley's misconduct, including its failure to comply with applicable standards, when viewed objectively from Morgan Stanley's standpoint at the time of the conduct, involved an extreme degree of risk, considering the probability and magnitude of the potential harm to others, and Morgan Stanley was aware of the risk involved, but nevertheless proceeded with conscious indifference to the rights, safety, and/or welfare of others.

424. As a result of Morgan Stanley's reckless disregard for Plaintiffs' and Class Members' interests by failing to secure their PII despite knowing its protocols, policies, procedures, and practices were not adequately designed, implemented, maintained, monitored, and tested, Plaintiffs and Class Members suffered injury, which includes, but is not limited to, impermissible release, disclosure, and publication—both directly and indirectly by Morgan Stanley as well as unauthorized parties—of their PII as well as exposure to a heightened, imminent risk of fraud, identity theft, financial and other harm. Plaintiffs and Class Members must monitor their financial accounts and credit histories more closely and frequently to guard against identity theft. Plaintiffs and Class Members also have incurred, and will continue to incur on an indefinite basis, out-of-pocket costs for obtaining credit reports, credit freezes, credit monitoring services, and other protective measures to deter or detect identity theft. The

impermissible release, disclosure, and publication of Plaintiffs' and Class Members' PII has also diminished the value of their PII.

425. The harm to Plaintiffs and the Class members was a proximate and reasonably foreseeable result of Morgan Stanley's breach of its duty of reasonable care in safeguarding Class Members' PII.

426. Morgan Stanley has engaged in conduct entitling Plaintiffs and Class Members to an award of punitive damages pursuant to common law principles and the statutory provisions of the State of New York.

427. Morgan Stanley's conduct as described herein shows willful misconduct, malice, fraud, wantonness, oppression, or that entire want of care which raises the presumption of conscious indifference to consequences, thereby justifying an award of punitive damages.

428. Plaintiffs therefore will seek to assert claims for punitive damages at the appropriate time under governing law in an amount within the jurisdictional limits of the Court.

429. Plaintiffs also allege that the acts and omissions of Morgan Stanley constitute gross negligence that proximately caused the injuries to Plaintiffs and Class Members. In that regard, Plaintiffs will seek punitive damages in an amount that would punish Morgan Stanley for its conduct, and which would deter other financial institutions from engaging in such misconduct in the future.

COUNT III
Violations of New York Consumer Law for Deceptive Acts and Practices New York Gen. Bus. Law § 349
(On Behalf of Plaintiffs and the Class)

430. All Plaintiffs, individually and on behalf of the Class, or, in the alternative New York Plaintiffs, individually and on behalf of the New York Subclass, re-allege and incorporate by reference paragraphs 1-354 and 371-380 as though fully alleged herein.

431. New York General Business Law ("NYGBL") § 349 prohibits deceptive acts or practices in the conduct of any business, trade, or commerce, or in the furnishing of any service in the state of New York.

432. By reason of the conduct alleged herein, Morgan Stanley has engaged in unlawful practices within the meaning of the NYGBL § 349. The conduct alleged herein is a "business practice" within the meaning of the NYGBL § 349, and the deception occurred within New York State.

433. Morgan Stanley stored Plaintiffs' and Class Members' PII on the aforementioned servers. Morgan Stanley knew or should have known it did not employ reasonable, industry standard, and appropriate security measures that complied "with federal regulations" and that would have kept Plaintiffs' and Class Members' PII secure and prevented the loss or misuse of Plaintiffs' and Class Members' PII. Morgan Stanley did not disclose to Plaintiffs and Class Members that the disposal of the servers was not in a secure manner.

434. Plaintiffs and Class Members never would have provided their sensitive and personal PII if they had been told or knew that Morgan Stanley would fail to maintain sufficient security to keep such PII from being taken by others.

435. Morgan Stanley violated NYGBL §349 by misrepresenting, both by affirmative conduct and by omission, the safety of Morgan Stanley's storage and services, specifically the security thereof, and its ability to safely store and dispose of Plaintiffs' and Class Members' PII.

436. Morgan Stanley also violated NYGBL §349 by failing to implement reasonable and appropriate security measures or follow industry standards for data security, and by failing to immediately notify Plaintiffs and Class Members of the Data Security Incidents. If Morgan

Stanley had complied with these legal requirements, Plaintiffs and Class Members would not have suffered the damages related to the Data Security Incidents.

437. Morgan Stanley's practices, acts, policies, and course of conduct violate NYGBL § 349 in that:

a. Morgan Stanley actively and knowingly misrepresented or omitted disclosure of material information to Plaintiffs and Class Members at the time they provided such PII that Morgan Stanley did not have sufficient security or mechanisms to protect PII;

b. Morgan Stanley failed to give timely warnings and notices regarding the defects and problems with the disposal of its serves to protect Plaintiffs' and Class Members' PII. Morgan Stanley possessed prior knowledge of the inherent risks in its disposal practices.

438. Plaintiffs and the Class were entitled to assume, and did assume, Morgan Stanley would take appropriate measures to keep their PII safe. Morgan Stanley did not disclose at any time that Plaintiffs' and Class Members' PII was vulnerable to malicious actors due to Morgan Stanley's asset disposal practices, and Morgan Stanley was the only one in possession of that material information, which it had a duty to disclose.

439. The aforementioned conduct constitutes an unconscionable commercial practice in that Morgan Stanley has, by the use of false or deceptive statements and/or knowing intentional material omissions, misrepresented and/or concealed the inadequate nature of its disposal practices, resulting in the Data Security Incidents.

440. Members of the public were deceived by Morgan Stanley's misrepresentations and failures to disclose.

441. Such acts by Morgan Stanley are and were deceptive acts or practices which are and/or were likely to mislead a reasonable consumer providing his or her PII to Morgan Stanley.

Said deceptive acts and practices are material. The requests for and use of such PII in New York through deceptive means occurring in New York were consumer-oriented acts and thereby falls under the New York consumer fraud statute, NYGBL § 349.

442. Morgan Stanley's wrongful conduct caused Plaintiffs and Class Members to suffer a consumer-related injury by causing them to incur substantial expense to protect from misuse of the PII by third parties and placing the Plaintiffs and Class Members at serious risk for monetary damages.

443. As a direct and proximate result of Morgan Stanley's violations of the above, Plaintiffs and Class Members suffered damages including, but not limited to:

a. unauthorized use of their PII;

b. theft of their personal and financial information;

c. costs associated with the detection and prevention of identity theft and unauthorized use of their financial accounts;

d. damages arising from the inability to use their PII;

e. loss of use of and access to their account funds and costs associated with the inability to obtain money from their accounts or being limited in the amount of money they were permitted to obtain from their accounts, including missed payments on bills and loans, late charges, and fees, and adverse effects on their credit including decreased credit scores and adverse credit notations;

f. costs associated with time spent and the loss of productivity or the enjoyment of one's life from taking time to address an attempt to ameliorate, mitigate and deal with the actual and future consequences of the Data Security Incidents, including finding fraudulent charges, purchasing credit monitoring and identity theft protection services,

initiating and monitoring credit freezes, and the stress, nuisance, and annoyance of dealing with all issues resulting from the Data Security Incidents;

g. the imminent and certainly impending injury flowing from potential fraud and identity theft posed by their PII being placed in the hands of criminals;

h. damages to and diminution in value of their PII entrusted to Morgan Stanley; and

i. the loss of Plaintiffs' and Class Members' privacy.

444. In addition to or in lieu of actual damages, because of the injury, Plaintiffs and the Class seek statutory damages for each injury and violation that has occurred.

COUNT IV
Breach of Fiduciary Duty
(On Behalf of Plaintiffs and the Class)

445. Plaintiffs re-allege and incorporate by reference paragraphs 1-354 and 371-380 as though fully alleged herein.

446. In order to establish and maintain Morgan Stanley accounts, Plaintiffs and Class Members were required to provide Morgan Stanley with a broad range of PII. Morgan Stanley in turn, was provided access to all such PII, which Morgan Stanley stored and maintained, purportedly in confidence, and which Morgan Stanley was required to strictly maintain in confidence without public access or other disclosure absent Plaintiffs' and Class Members' written consent.

447. Morgan Stanley owed and continues to owe a fiduciary duty to Plaintiffs and Class Members. By virtue of its position as a financial institution, which gave Morgan Stanley wide-ranging access to Plaintiffs' and Class Members' PII, and because of Morgan Stanley's superior knowledge, business responsibilities, and duties—including those provided by law or statute—and its unlimited control over Plaintiffs' and Class members' PII in its IT Assets,

Morgan Stanley assumed a fiduciary duty to Plaintiffs and Class Members to secure and maintain that PII, free from unauthorized disclosure.

448. As a result of this relationship of trust and confidence, the highly confidential nature of Plaintiffs' and Class Members' PII, and Morgan Stanley's duties and obligations respecting maintaining the privacy of such information, Morgan Stanley owed to Plaintiffs and Class Members the highest degree of loyalty, honesty, fidelity, trust, and due care in its fiduciary obligations with respect to securing and maintaining the privacy of their PII. In order to comply with such duty, Morgan Stanley was required to exercise diligence to protect and secure that PII from unauthorized access, fraud, or theft and to take all necessary steps in order to do so, including encrypting that PII and properly disposing of any IT Assets on which it was stored.

449. Morgan Stanley breached its fiduciary duty to Plaintiffs and Class Members by failing to take all adequate and necessary steps to maintain the confidentiality and privacy of their PII.

450. Morgan Stanley independently breached its fiduciary duty to Plaintiffs and Class Members by failing to timely and adequately disclose that it had not taken the necessary steps to protect that PII from unauthorized access and theft and that the PII was at a heightened risk of being divulged by virtue of Morgan Stanley's data security failings and policies.

451. Morgan Stanley independently breached its fiduciary duty to Plaintiffs and Class Members by placing its own interest in avoiding expense ahead of the privacy and data security interests of Plaintiffs and Class Members.

452. As a direct and proximate result of Morgan Stanley's breach of fiduciary duty, Plaintiffs and Class Members have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the inherent value of their PII; (iii) the divulgence,

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 Security Incidents, 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 Morgan Stanley's possession and is subject to further unauthorized disclosures so long as Morgan Stanley fails to undertake appropriate and adequate measures to protect the PII of 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 divulged as a result of the Data Security Incidents for the remainder of the lives of Plaintiffs and Class Members; (ix) the diminished value of Morgan Stanley's goods and services they received; and (x) nominal damages.

453. As a direct and proximate result of Morgan Stanley's breach of fiduciary duty, Plaintiffs and Class Members have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

454. Additionally, as a direct and proximate result of Morgan Stanley's fiduciary duty, Plaintiffs and Class members have suffered and will suffer the continued risks of exposure of their PII, which remain in Morgan Stanley's possession and is subject to further unauthorized disclosures so long as Morgan Stanley fails to undertake appropriate and adequate measures to protect the PII in its continued possession.

COUNT V
Unjust Enrichment
(On Behalf of Plaintiffs and the Class)

455. Plaintiffs re-allege and incorporate by reference paragraphs 1-354 and 371-380 as though fully alleged herein.

456. Plaintiffs plead this claim in the alternative to their common law and statutory claims alleged herein.

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

458. Morgan Stanley appreciated or had knowledge of the benefits conferred upon it by Plaintiffs and Class Members and it accepted and retained that benefit. Morgan Stanley profited from the purchases and used the PII of Plaintiffs and Class Members for business purposes.

459. Plaintiffs' and Class Members' PII was private and confidential, and its value depended upon Defendant maintaining the privacy and confidentiality of that PII.

460. The monetary amounts Plaintiffs and Class Members paid for Morgan Stanley'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 Plaintiffs' and Class Members' PII.

461. Under the principles of equity and good conscience, Morgan Stanley should not be permitted to retain the money belonging to Plaintiffs and Class Members, because Morgan

Stanley failed to implement the data management and security measures that are mandated by industry standards.

462. Morgan Stanley failed to secure the PII of Plaintiffs and Class Members and, therefore, did not provide full compensation for the benefit Plaintiffs and Class Members provided.

463. Morgan Stanley acquired the PII through inequitable means in that it failed to disclose the inadequate security practices previously alleged.

464. If Plaintiffs and Class Members knew that Morgan Stanley would not secure their PII using adequate security, they would not have made purchases or developed a financial relationship with Morgan Stanley.

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

466. As a direct and proximate result of Morgan Stanley's conduct, Plaintiffs and Class Members have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the inherent value of their PII; (iii) the divulgence, 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 Security Incidents, 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 Morgan Stanley's possession and is subject to further unauthorized disclosures so long as Morgan Stanley 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 divulged as a result of the Data Security Incidents for the remainder of the lives of Plaintiffs and Class Members; (ix) the diminished value of Morgan Stanley's goods and services they received; and (x) nominal damages.

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

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

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

469. Plaintiffs re-allege and incorporate by reference paragraphs 1-354 and 371-380 as though fully alleged herein.

470. At all times during Plaintiffs' and Class Members' interactions with Morgan Stanley, Morgan Stanley was fully aware of the confidential and sensitive nature of Plaintiffs' and Class Members' PII that Plaintiffs and Class Members provided to Morgan Stanley.

471. As alleged herein and above, Morgan Stanley's relationship with Plaintiffs and Class Members was governed by terms and expectations that Plaintiffs' and Class Members' PII

would be collected, stored, and protected in confidence, and would not be disclosed to unauthorized third parties.

472. Plaintiffs and Class Members provided their respective PII to Morgan Stanley with the explicit and implicit understandings that Morgan Stanley would protect and not permit the PII to be disseminated to any unauthorized third parties.

473. Plaintiffs and Class Members also provided their respective PII to Defendant with the explicit and implicit understandings that Morgan Stanley would take precautions to protect that PII from unauthorized disclosure.

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

475. Due to Morgan Stanley's failure to prevent the Data Security Incidents from occurring, Plaintiffs' and Class Members' PII was disclosed and misappropriated to unauthorized third parties beyond Plaintiffs' and Class Members' confidence, and without their express permission.

476. As a direct and proximate cause of Morgan Stanley's actions and/or omissions, Plaintiffs and Class Members have suffered damages.

477. But for Morgan Stanley's disclosure of Plaintiffs' and Class Members' PII in violation of the parties' understanding of confidence, their PII would not have been divulged, compromised, stolen, viewed, accessed, and used by unauthorized third parties. Morgan Stanley's breaches were the direct and legal cause of the theft of Plaintiffs' and Class Members' PII, as well as the resulting damages.

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

479. As a direct and proximate result of Morgan Stanley's' breach of its confidence with Plaintiffs and Class Members, Plaintiffs and Class Members have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the inherent value of their PII; (iii) the divulgence, 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 Security Incidents, 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 Morgan Stanley's possession and is subject to further unauthorized disclosures so long as Morgan Stanley fails to undertake appropriate and adequate measures to protect the PII of customers/patients and former customers/patients 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 divulged as a result of the breaches for the remainder of the lives of Plaintiffs and Class Members; (ix) the diminished value of Morgan Stanley's goods and services they received; and (x) nominal damages.

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

PRAYER FOR RELIEF

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

A. An Order certifying the Class as defined above, and appointing Plaintiffs and their Counsel to represent the certified Class;

B. Equitable relief enjoining Morgan Stanley from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiffs' and Class Members' PII, and from refusing to issue prompt, complete, any accurate disclosures to Plaintiffs and Class Members;

C. Equitable relief compelling Morgan Stanley to use appropriate cyber security methods and policies with respect to PII collection, storage, protection, and disposal, and to disclose with specificity to Plaintiffs and Class Members the type of PII divulged;

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

E. An award of punitive damages;

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

G. Prejudgment interest on all amounts awarded; and

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

DEMAND FOR JURY TRIAL

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

Date: July 5, 2021

Respectfully submitted,

NUSSBAUM LAW GROUP, P.C.

By: */s/ Linda P. Nussbaum*
Linda P. Nussbaum
Bart D. Cohen
Marc E. Foto
1211 Avenue of the Americas, 40th Fl.
New York, NY 10036
(917) 438-9189
lnussbaum@nussbaumpc.com
bcohen@nussbaumpc.com
mfoto@nussbaumpc.com

MORGAN & MORGAN

By: */s/ Jean Martin*
Jean S. Martin
Ryan J. McGee
Francesca Kester
201 N. Franklin Street, 7th Floor
Tampa, Florida 33602
(813) 223-5505
jmartin@ForThePeople.com
rmcgee@ForThePeople.com
fkester@ForThePeople.com

Interim Co-Lead Counsel for Plaintiffs

UNITED STATES DISTRICT COU
FOR THE SOUTHERN DISTRICT OF N

In re Morgan Stanley Data Security Litigation	20 Civ. 5914 (AT)

STIPULATION AND SCHEDULING ORDER REGARDING
PLAINTIFFS' SECOND CONSOLIDATED AMENDED COMPLAINT

Plaintiffs Mark Blythe, Cheryl Gamen, Richard Gamen, Amresh Jaijee, Howard Katz, Richard Mausner, John Nelson, Midori Nelson, Desiree Shapouri, Sylvia Tillman, and Vivian Yates (collectively, "Plaintiffs"), and Defendant Morgan Stanley Smith Barney, LLC ("Morgan Stanley" or "Defendant") hereby stipulate and agree as follows:

WHEREAS, on November 2, 2020, Plaintiffs filed a Consolidated Class Action Complaint (ECF No. 38);

WHEREAS, on January 14, 2021, Defendant filed a Motion to Dismiss the Consolidated Class Action Complaint Pursuant to Rules 12(b)(1) and 12(b)(6) (ECF 47) ("Motion to Dismiss");

WHEREAS, pursuant to the Court's Order of March 1, 2021 (ECF 53), Section III.B.iv of the Court's Individual Practices in Civil Cases, and Rule 15(a)(1)(B) of the Federal Rules of Civil Procedure, Plaintiffs are required to file either a response to Defendant's Motion to Dismiss, or a Second Consolidated Class Action Complaint no later than June 4, 2021;

WHEREAS, Plaintiffs and Defendant held a mediation before the Honorable Diane M. Welsh (Ret.) of JAMS on May 24, 2021, and have scheduled a second mediation for July 2, 2021 (the "Mediation");

WHEREAS, Plaintiffs and Defendant are engaged in party and non-party discovery; and

WHEREAS, Plaintiffs intend to serve a Second Consolidated Class Action Complaint rather than responding to Defendants' Motion to Dismiss.

IT IS HEREBY STIPULATED AND AGREED, subject to the Court's approval, that:

1. Plaintiffs' above-referenced June 4, 2021 deadline is adjourned until **July 5, 2021,** to allow the parties to continue discovery and proceed with the Mediation; and

2. Plaintiffs and Defendant shall agree on a subsequent schedule for briefing the Motion to Dismiss, subject to the Court's approval.

3. The deadline to complete all fact discovery is adjourned to October 29, 2021;

4. The deadline to serve interrogatories is adjourned to August 20, 2021;

5. The deadline to serve requests is adjourned to September 28, 2021; and

6. The deadline to complete all expert discovery is adjourned to January 7, 2022.

STIPULATED and AGREED to this 27th day of May, 2021.

Respectfully submitted,

MORGAN & MORGAN

By: */s/ Jean Martin*
Jean Martin
201 N. Franklin Street, 7th Floor
Tampa, Florida 33602
(813) 223-5505
jmartin@ForThePeople.com

NUSSBAUM LAW GROUP, P.C.

By: */s/ Linda P. Nussbaum*
Linda P. Nussbaum
1211 Avenue of the Americas, 40th Fl.
New York, NY 10036
(917) 438-9189
lnussbaum@nussbaumpc.com

Interim Co-Lead Counsel for Plaintiffs

PAUL, WEISS, RIFKIND, WHARTON & GARRISON, LLP

By: */s/ Susanna M. Buergel*
Susanna M. Buergel
1285 Avenue of the Americas
New York, NY 10019
(212) 373-3000
sbuergel@paulweiss.com

PAUL, WEISS, RIFKIND, WHARTON & GARRISON, LLP

By: */s/ Jane Baek O'Brien*
Jane Baek O'Brien
2001 K Street, N.W.
Washington, DC 20006
(202) 223-7300
jobrien@paulweiss.com

Attorneys for Defendant Morgan Stanley Smith Barney LLC

SO ORDERED.

Dated: June 1, 2021
New York, New York

ANALISA TORRES
United States District Judge