GLANCY PRONGAY & MURRAY LLP
LIONEL Z. GLANCY (#134180)
MARC L. GODINO (#182689)
MARK S. GREENSTONE (#199606)
1925 Century Park East, Suite 2100
Los Angeles, CA 90067
Telephone: (310) 201-9150
Facsimile: (310) 201-9160
E-mail: info@glancylaw.com

Counsel for Plaintiffs
[Additional Counsel Listed On Signature Page]

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

EVERETT CASTILLO, LINDA CASTILLO, NICHOLAS DATTOMA, FREDA LANG, WENDY TRAN, AND STEVEN WILK, INDIVIDUALLY AND ON BEHALF OF ALL OTHERS SIMILARLY SITUATED,

Plaintiffs,

v.

SEAGATE TECHNOLOGY, LLC,

Defendant.

Case No.: 3:16-cv-01958-RS

FIRST AMENDED CONSOLIDATED CLASS ACTION COMPLAINT

JURY TRIAL DEMANDED

Everett Castillo, Linda Castillo, Nicholas Dattoma, Freda Lang, Wendy Tran and Steven Wilk ("Plaintiffs"), individually and on behalf of all others similarly situated, file this Consolidated Class Action Complaint against Seagate Technology, LLC ("Seagate"[1]) and allege the following based on personal knowledge, the investigation of counsel, and information and belief.

INTRODUCTION

1. Plaintiffs and the other Class Members are current and former employees or spouses of Defendant who entrusted their personally identifiable information ("PII") to Seagate. Defendant betrayed Plaintiffs' trust by failing to properly safeguard and protect their PII and disclosed their PII to cybercriminals.

2. On or about March 1, 2016, a Seagate employee responded to an Internet "phishing"[2] scam by forwarding to unknown cybercriminals the 2015 Forms W-2 data for all of Seagate's and Seagate's affiliates' current and former employees ("Employees"). The Form W-2 data contained sensitive personally identifying information ("PII"), including, among other things, names, addresses, salaries and, most importantly, Social Security numbers. By disclosing its Employees' PII to cybercriminals (the "Data Breach"), Seagate put all of its

[1] As used herein, "Seagate" includes any Seagate affiliates and subsidiaries for which Seagate processed the Employees' 2015 Forms W-2 or for which Seagate possessed Employee Form W-2 data. Allegations that "Seagate" processed or provided an Employees' Form W-2, include Forms W-2 that were processed and/or distributed by Seagate's affiliates and subsidiaries.

[2] "Phishing" is an attempt to acquire PII by masquerading as a trustworthy entity through an electronic communication. *See* http://www.onguardonline.gov/articles/0003-phishing. Phishing is typically carried out by e-mail spoofing that looks like a legitimate email and often directs the recipient to provide PII. When criminals have access to PII from a large group of similarly situated victims, it is much more feasible to develop a believable phishing spoof email.

Employees at risk.

3. [redacted]

4. Almost immediately after the Data Breach, the cybercriminals exploited Seagate's wrongful actions and filed fraudulent federal and state tax returns in the names of Employees. Some Employees have learned that the cybercriminals filed fraudulent *joint* tax returns, using not only the Employee's Social Security number, but also the Employee's spouse's Social Security number ("Third-Party Victims"). In order for the cybercriminals to have obtained Employees' spouse's Social Security numbers, the disclosed PII likely contained more than just the Form W-2 data for Employees.

5. Seagate negligently failed to take the necessary precautions required to safeguard and protect Plaintiffs' and the other Class Members' PII from unauthorized disclosure resulting in Plaintiffs' and the other Class Members' PII being readily copied by data thieves. Defendant's actions represent a flagrant disregard of Plaintiffs' and the other Class Members' rights, both as to privacy and property.

6. Employees and Third-Party Victims are now, and for the rest of their lives will be, at a heightened risk of identity theft. As a direct result of the Data Breach, many Employees and Third-Party Victims have already suffered out-of-pocket costs attempting to rectify fraudulent tax returns and engaging services to monitor and protect their identity and credit. Employees and Third-Party Victims will continue to suffer out-of-pocket costs in the future to

protect and, if necessary, repair their credit and identity. By this action, Plaintiffs seek to hold Seagate responsible for the harm caused by its negligence.

7. Plaintiffs bring this action because as a direct and/or proximate result of Defendant's wrongful actions and/or inaction and the resulting Data Breach, Plaintiffs have incurred (and will continue to incur) damages in the form of, *inter alia*, (i) loss of privacy and/or (ii) the additional damages set forth in detail below, which are incorporated herein by reference.

8. As a direct and/or proximate result of Defendant's wrongful actions and/or inaction and the resulting Data Breach, Plaintiffs and the other Class Members have been deprived of the value of their PII, for which there is a well-established national and international market. For example, stolen PII is sold on the cyber black market for $14 to $25 per record to individuals focused on committing fraud or needing or wanting a new identity.

9. Defendant's wrongful actions and/or inaction and the resulting Data Breach have also placed Plaintiffs and the other Class Members at an imminent, immediate and continuing increased risk of identity theft and identity fraud. Indeed, Javelin Strategy & Research ("Javelin"), a leading provider of quantitative and qualitative research, released its 2015 Identity Fraud Report ("the Javelin Report"), quantifying the impact of data breaches. According to the Javelin Report, individuals whose PII is subject to a reported data breach are approximately 9.5 times more likely than the general public to suffer identity fraud and/or identity theft. Moreover, there is a high likelihood that significant identity fraud and/or identity theft has not yet been discovered or reported, and a high probability that criminals who may now possess Plaintiffs' and the other Class Members' PII and not yet used the information will do so at a later date or re-sell it.

10. Plaintiffs on behalf of themselves and the other Class Members, seeks actual damages, economic damages, injunctive relief, and attorneys' fees, litigation expenses, and costs.

JURISDICTION AND VENUE

11. This Court has jurisdiction over the claims in this action pursuant to 28 U.S.C. § 1332(d) because there are more than 100 Class Members, at least one Class Member is a citizen of a state that is diverse from Seagate, and the amount in controversy exceeds $5 million, exclusive of interest and costs.

12. This Court has personal jurisdiction over Seagate because Seagate maintains its principal place of business in this District, is registered to conduct business in California, and has sufficient minimum contacts with California.

13. Venue is proper in this District pursuant to 28 U.S.C. § 1391(b) because Seagate resides in this District and a substantial part of the events or omissions giving rise to Plaintiffs' claims occurred in this District.

PARTIES

14. Plaintiff Everett Castillo is a resident of California and an Employee. In 2015, Mr. Castillo was employed by Lyve Minds, Inc. ("Lyve"). Lyve was acquired by Seagate during 2015 and maintained as a Seagate subsidiary. Although Mr. Castillo received his 2015 Form W-2 from Lyve, Seagate had Mr. Castillo's Form W-2 data. Seagate informed Mr. Castillo that Seagate had disclosed his Form W-2 data in the Data Breach.

15. Plaintiff Linda Castillo is a resident of California and is married to Mr. Castillo. Linda Castillo did not work for Seagate or one of its affiliates. Ms. Castillo is a Third-Party Victim.

16. Plaintiff Nicholas Dattoma is a resident of Oceano, California and a former employee of Seagate Technology, LLC. Mr. Dattoma was employed by Seagate during 2015 and received a Form W-2 from Seagate for 2015. Seagate informed Mr. Dattoma that Seagate had disclosed his Form W-2 data in the Data Breach.

17. Plaintiff Freda Lang resides in Oklahoma City, Oklahoma is a current Seagate employee. Seagate informed Ms. Lang that her Form W-2 Data was disclosed in the Data Breach.

18. Plaintiff Wendy Tran is a resident of California and an Employee. In 2015, Ms. Tran was employed by Lyve, which was acquired by Seagate during 2015. Although Ms. Tran received her 2015 Form W-2 from Lyve, Seagate had Ms. Tran's Form W-2 data. Seagate informed Ms. Tran that Seagate had disclosed her Form W-2 data in the Data Breach.

19. Plaintiff Steven Wilk is resident of Dana Point, California. Mr. Wilk is a former Seagate employee and learned of the Data Breach through a letter sent by Defendant. Mr. Wilk's state and federal tax returns were fraudulently filed on his behalf.

20. Defendant Seagate Technology, LLC is a limited liability corporation organized under the laws of the state of Delaware with its principal place of business in Cupertino, California.

FACTUAL ALLEGATIONS

21. Data security breaches – and data security breach litigation – dominated the headlines in 2015 and continue to do so in 2016. Continuous widely publicized breaches have led to 30,000 articles a *month* being published that reference data breach litigation. Law firms

have collectively published more than 156,000 articles on the topic.[3]

22. According to the Privacy Rights Clearinghouse Chronology of Data Breaches, 282 breaches were publicly reported during the fourth quarter of 2014 through the fourth quarter of 2015.[4]

23. Seagate's own website recognizes the recent uptick in data breaches. For example:

- "The importance of protecting information stored in data centers has risen in prominence alongside news of high-profile breaches."[5]
- "Although the IT industry pays a lot of attention to external attacks, organizations are comparably worried about malicious insiders. When asked about the greatest security risks they face, 53% of respondents said cyber criminals, while 51% cited authorized users." *Id*.
- "According to industry experts such as the Ponemon Institute, the average cost per data breach increases every year, and on average was US $6.6 million in 2008, or US $202 per compromised record."[6]

24. Seagate even contains a "cautionary note" in its public SEC filings that certain statements made by Seagate involve a number of known and unknown risks, uncertainties, and

[3] Google News Search for "Data Breach Litigation" conducted on March 22, 2016 (covers 30 days); Lexology.com search for "Data Breach Litigation" conducted on March 25, 2016.
[4] *See* Privacy Rights Clearinghouse Chronology of Breaches *available at* http://www.privacyrights.org.
[5] http://www.seagate.com/tech-insights/data-center-management-master-ti/
[6] http://www.seagate.com/tech-insights/fips-140-2-standard-and-self-encrypting-drive-technology-master-ti/

other factors including "cyber-attacks or other data breaches that disrupt its operations or results in the dissemination of proprietary or confidential information."[7]

25. Seagate announced on or about March 1, 2016, that it discovered that it was the victim of a "phishing" scam (the "Data Breach"). According to Seagate, the Data Breach resulted in the release of PII for approximately 10,000 of its and its affiliates' current and former employees. In the Data Breach, Seagate provided to unknown cybercriminals the 2015 Forms W-2 data for all Employees. The Form W-2 data disclosed the Employees' names, addresses, compensation and, most importantly, Social Security numbers.

26. [redacted] Almost immediately, the cybercriminals began to exploit the Employees' PII by, *inter alia*, filing false federal and state tax returns for some or all of the Employees. In some cases, the cybercriminals filed joint tax returns, on behalf of an Employee and his or her spouse. The false joint tax returns used the Employee's spouse's Social Security number. Form W-2 data does not contain the Social Security number for spouses. The fact that the cybercriminals had obtained the Social Security number for at least some of the Employees' spouses suggests that the Data Breach involved more information than just Form W-2 data.

27. Other Seagate employees also reported having credit cards fraudulently opened in their names shortly after the Data Breach. [redacted]

[7] http://www.seagate.com/about-seagate/news/seagate-technology-announces-preliminary-financial-information-for-fiscal-third-quarter-2016/

[redacted]

28. [redacted]

[redacted]

29. [redacted]

[redacted]

30. The cybercriminals who obtained the Employees' and Third-Party Victims' PII may continue to exploit the data themselves and/or sell the data in the so-called "dark markets." Having obtained the Employees' and Third-Party Victims' names, addresses and Social Security numbers, cybercriminals can pair the data with other available information to commit a broad range of fraud in an Employee's name, including but not limited to:

a. obtaining employment;

b. obtaining a loan;

c. applying for credit cards or spending money;

d. filing false tax returns;

e. obtaining medical care;

f. stealing Social Security and other government benefits; and

g. applying for a driver's license, birth certificate or other public document.

31. In addition, if an Employee's or Third-Party Victims' Social Security number is used to create a false identification for someone who commits a crime, the Employee or Third-Party Victim may become entangled in the criminal justice system, impairing the Employee's or Third-Party Victim's ability to gain employment or obtain a loan.

32. For the rest of their lives, Plaintiffs and the class members will bear an immediate and heightened risk of all manners of identity theft.

33. Seagate itself recognizes the extensive damage that the Data Breach can cause its employees. [redacted]

34. By the time current and former employees received notice of the Data Breach, many were already the victims of identity theft.

35. This is not the first time Seagate has been the target of a phishing scam. [redacted]

36. [redacted]

37. [redacted]

38. [redacted]

39. In addition, just prior to the Data Breach, Internet security researcher Brian Krebs warned of this precise scam on his Internet website. Krebs warned that as tax season approached Internet scammers were trying to scam various companies by sending false emails, purportedly from the company's chief executive officer, to individuals in the human resources and accounting departments and asking for copies of Forms W-2 data.[8]

40. Seagate's negligence in safeguarding the Employees' and Third-Party Victims' PII is exacerbated by the fact that the company's own website recognizes the threat of data breaches. For example, Seagate claims that "[a]s the volume of data continues to grow exponentially, the risk of a costly data breach increases with it, and organizations should not wait until such a breach occurs before committing to a solution."[9] Seagate also claims on its website that "**Data Security** Data breaches, regulations with encryption *Safe Harbor* provisions and lawsuits from lost data all underscore why companies must safeguard their data."[10]

---

[8] "Phishers Spoof CEO, Request W2 Forms," Krebsonsecurity.com. http://bit.ly/25oAc2c.
[9] http://www.seagate.com/tech-insights/self-encrypting-drive-tech-tco-master-ti/
[10] http://www.seagate.com/tech-insights/unified-storage-architecture-master-ti/

41. Seagate even touts the high level of security and encryption features available with its own products. For example, Seagate's website describes the security features for its hard drives:

> Secure your data with Seagate's portfolio of Self-Encrypting Drives (SED) for enterprise and PCs with options like Seagate Instant Secure Erase (ISE) for painless drive retirement and the world's only FIPS 140-2 validated hard drive solution. Choose the level of 'data-at-rest' security that's right for you. Seagate Secure™ Technology[11]

42. Seagate conceded its fault in the Data Breach. Seagate's Chief Financial Officer wrote in a March 4, 2016 email to employees: "This mistake was caused by human error and lack of vigilance, and could have been prevented."

Seagate's Current and Former Employees and the Third-Party Victims Have Suffered Concrete Injury

43. As part of their employment, the Employees were required to provide Seagate with sensitive personal information, including their Social Security numbers. In addition, in order to obtain certain benefits, such as retirement or insurance benefits, Employees must provide Seagate with PII for their beneficiaries as well. Seagate had a duty to protect that information against wrongful disclosure to third parties. Seagate failed to comply with its duties to its current and former employees and their beneficiaries by failing to implement policies and procedures to prevent cybercriminals and scammers from obtaining the Employees' and Third-Party Victims' PII.

44. As a result of the Data Breach, numerous Employees and Third-Party Victims have already suffered damages. In addition, the disclosure of an individual's Social Security number puts one at great risk of future fraudulent conduct. By pairing a Social Security number

[11] http://www.seagate.com/solutions/security/

with someone's name, address and, perhaps, other readily available information, an identity thief can commit a broad range of fraud, including but not limited to a) obtaining unemployment; b) obtaining a loan; c) applying for credit cards or spending money under the victim's name; d) filing false tax returns; e) obtaining medical care; f) stealing Social Security and other government benefits; and g) applying for a driver's license, birth certificate or other public document. Any of these activities can cause significant financial and emotional harm to a victim. Even if the victim applies for and receives a replacement Social Security number, he or she will not be free from risk.

45. Plaintiff Tran is an Employee whose 2015 Form W-2 data was disclosed by Seagate. Ms. Tran provided confidential information to Seagate including her name, date of birth and social security number in connection with her employment. Ms. Tran reasonably expected that Seagate would maintain the privacy of her confidential PII. When Ms. Tran learned about the Data Breach, she promptly investigated and learned that both a fraudulent federal tax return and a fraudulent state tax return had been filed on her behalf. Ms. Tran learned that the fraudulent federal tax return was dated March 3, 2016 – just two days after Seagate announced the Data Breach.

46. Although Ms. Tran usually prepares and files her federal and state tax returns on her own, she retained the services of an accountant to assist with redressing the fraudulent tax returns and filing her 2015 federal and state returns. Ms. Tran has incurred additional costs with respect to the accountant that she would not have had to pay, but for the Data Breach.

47. Ms. Tran has spoken with individuals at the California Franchise Tax Board to determine what she must do to file her state returns going forward, and she has received different advice. One individual told her that she cannot e-file her state taxes for the foreseeable

future. Another individual told her that she can e-file, but if she is getting a state tax refund, she must call a certain telephone number to confirm the refund before the state will release it. As of September 1, 2016, Ms. Tran still had not received her 2015 federal tax return.

48. Although Seagate offered Ms. Tran (along with other Employees) two years of limited identity theft protection through Experian's ProtectMyID service, Ms. Tran is unable to take advantage of this service. Ms. Tran already has a subscription to ProtectMyID because she was a victim of a prior unrelated data breach.

49. In or around September 2015, Ms. Tran received notification that Experian, which processed credit applications for T-Mobile, had experienced a data breach in which information concerning certain T-Mobile customers was disclosed. However, Ms. Tran was not informed that any of her personal information had been disclosed in T-Mobile data breach; and she did not suffer any identity theft until after the Seagate Data Breach. Nonetheless, T-Mobile offered her two years of ProtectMyID service, which she accepted. When Ms. Tran attempted to sign-up for the ProtectMyID service offered by Seagate, Experian informed Ms. Tran that she cannot create a second subscription. Further, her current ProtectMyID subscription will lapse in a few months' time – but not until after the deadline for signing up for the Seagate sponsored ProtectMyID service. Ms. Tran is effectively unable to obtain any relief from Seagate.

50. Plaintiff Everett Castillo is an Employee whose 2015 Form W-2 data was disclosed by Seagate. Plaintiff Linda Castillo is Mr. Castillo's wife. Mr. Castillo provided confidential information to Seagate including his and his wife's name, date of birth and social security number in connection with his employment. The Castillos reasonably expected that Seagate would maintain the privacy of their confidential PII. Soon after learning of the Data Breach, the Castillos investigated whether false tax returns had been filed on their behalf. They

learned that a fraudulent joint federal tax return had been filed on their behalf. The fraudulent tax returns contained both Mr. Castillo's Social Security number and Ms. Castillo's Social Security number. Ms. Castillo, however, never worked for Seagate or one of its affiliates and did not receive a Form W-2 from Seagate.

51. The Castillos have spent many hours attempting to have the fraudulent tax return withdrawn and investigating what steps they should take in response to the Data Breach. The Castillos have been informed by the California Franchise Tax Board that they cannot e-file their state tax return. The Castillos are considering purchasing an identity theft protection service that will provide real-time monitoring of their accounts and Social Security number. Although Seagate has offered Mr. Castillo two years of limited identity theft protection services, Seagate has not offered any protection to Ms. Castillo or offered to reimburse Ms. Castillo for any future identity theft and associated costs arising out of the Data Breach. Nor has Seagate offered to reimburse the Castillos for the time spent addressing the fraudulent tax return filed on their behalf.

52. Plaintiff Nicholas Dattoma is a former Employee whose 2015 Form W-2 data was disclosed by Seagate. Mr. Dattoma provided confidential information to Seagate including his name, date of birth and social security number in connection with his employment. Mr. Dattoma reasonably expected that Seagate would maintain the privacy of his confidential PII. He received a letter from Seagate in mid-March 2016 regarding the Data Breach, and he was also alerted of the Data Breach by former colleagues. On or about April 13, 2016, Mr. Dattoma's electronically filed 2015 federal and state tax returns were rejected because tax return documentation had already been filed using his PII. Mr. Dattoma has since taken the time and effort to re-file paper copies of his state and local taxes along with accompanying affidavits.

Additionally, Mr. Dattoma purchased identity theft protection and monitoring from Lifelock. Mr. Dattoma sought protection from LifeLock because Lifelock offered greater protection than the monitoring offered by Seagate.

53. Freda Lang is a current Seagate employee whose 2015 Form W-2 Data was disclosed by Seagate. She attempted to electronically file her federal taxes on April 17, 2016 and was informed that her return had already been filed. She contacted the IRS and was instructed to complete paperwork in connection with her claim. The IRS is currently investigating this matter and she was told it may take up to 180 days to resolve. Ms. Lang has been in contact with a third-party hired by Defendant in connection with the Data Breach.

54. Plaintiff Steven Wilk is a former Employee whose 2015 Form W-2 Data was disclosed by Seagate. Mr. Wilk provided confidential information to Seagate including his name, date of birth and social security number in connection with his employment. Mr. Wilk reasonably expected that Seagate would maintain the privacy of his confidential PII. Mr. Wilk learned of the Seagate Data Breach through a letter from the company. His 2015 federal tax returns were filed twice by unknown parities. Additionally, his 2015 state return was also filed by an unknown party. Mr. Wilk purchased identity theft protection and monitoring from Lifelock to protect his PII. Mr. Wilk sought protection from LifeLock because Lifelock offered greater protection than the monitoring offered by Seagate.

55. In addition, Plaintiffs, Employees and Third Party Victims will be at risk of identity theft for the rest of their lives, requiring constant diligence and monitoring. Upon information and belief, other Employees have suffered harm as a result of the Data Breach in addition to fraudulent tax returns and delays in receiving tax refunds.

Seagate's Inadequate Response to Protect the Employees and Third-Party Victims

56. Seagate has failed to provide adequate compensation for the Employees due to its negligence. Seagate has not offered any compensation to Third-Party Victims. To date, Seagate has offered Employees just two years of identity theft protection through the Experian ProtectMyID service. Even if an Employee accepts the ProtectMyID service, it will not provide Employees any compensation for the costs and burdens associated with the fraudulent tax returns that were filed prior to an Employee signing up for ProtectMyID. Seagate has not offered Employees any assistance in dealing with the IRS or state tax agencies. Nor has Seagate offered to reimburse Employees for the costs – current and future – incurred as a result of falsely filed tax returns.

57. The offered ProtectMyID service is inadequate to protect the Employees from the threats they face. It does nothing to protect *against* identity theft. Instead, it only provides a measure of assistance after identity theft has been discovered. For example, ProtectMyID only monitors Employees' *credit reports* – but fraudulent activity, such as the filing of a false tax return, may not appear on a credit report. ProtectMyID *does not* provide real time monitoring of Employees' credit cards and bank account statements. Employees must pay extra for that service. Although ProtectMyID offers up to $1 million of identity theft insurance, the coverage afforded is limited and often duplicative of (or inferior to) basic protections provided by banks and credit card companies. Thus, providing adequate identity theft protection is an essential component of the injunctive relief sought in this case.

58. Many websites that rank identity protection services are critical of ProtectMyID. NextAdvisor ranks ProtectMyID at the bottom of comparable services, noting that it "lacks in protection; only includes Experian credit report monitoring; 7-day trial for $1 with enrollment;

credit score and other credit reports cost extra." [12] BestIDtheftCompanys.com ranks ProtectMyID at No 30 with a score of just 4.4 out of 10 (and a "User Score" of just 1.3).[13]

CLASS ACTION ALLEGATIONS

59. Plaintiffs bring these claims pursuant to Federal Rule of Civil Procedure 23 on behalf of classes of similarly situated persons, which they propose to be defined as follows:

a. **Employee Class**: All current and former Seagate or Seagate affiliates' employees whose PII was compromised as a result of the Data Breach.

b. **Third-Party Class**: All non-current or non-former Seagate or Seagate affiliates' employees whose PII was compromised as a result of the Data Breach, including but not limited to spouses, children or other individuals associated with Employees.

60. **Numerosity**. The proposed class contains thousands of individuals dispersed throughout the United States. Joinder of all members is impracticable. Class members can be identified through Seagate's records.

61. **Commonality**. Common questions of fact and law exist for each cause of action and predominate over questions affecting only individual class members. Common questions include:

a. Whether and to what extent Seagate had a duty to protect the class members' PII;

b. Whether Seagate breached its duty to protect the class members' PII;

c. Whether Seagate disclosed class members' PII.

d. Whether Seagate timely, accurately, and adequately informed class members that their PII had been compromised;

[12] "Identity Theft Protection Reviews & Prices," NextAdvisor.com. http://bit.ly/1UCnsRP.
[13] "Experian ProtectMyID," bestidtesftcompanys.com. http://bit.ly/1Rh1YGy.

e. Whether class members are entitled to damages; and

f. Whether class members are entitled to injunctive relief.

62. **Typicality**. Plaintiffs' claims are typical of the claims of members of the proposed classes because, among other things, Plaintiffs and class members sustained similar injuries as a result of Seagate's uniform wrongful conduct; Seagate owed the same duty to each class member; and their legal claims arise from the same conduct by Seagate.

63. **Adequacy**. Plaintiffs will fairly and adequately protect the interests of the proposed classes. Their interests do not conflict with the class members' interests. Plaintiffs have retained class counsel experienced in class action litigation to prosecute this case on behalf of the classes.

64. **Rule 23(b)(3)**. In addition to satisfying the prerequisites of Rule 23(a), Plaintiffs satisfy the requirements for maintaining a class action under Rule 23(b)(3). Common questions of law and fact predominate over any questions affecting only individual class members and a class action is superior to individual litigation. The amount of damages available to individual class members is insufficient to make litigation addressing Seagate's conduct economically feasible in the absence of the class action procedure. Individualized litigation also presents a potential for inconsistent or contradictory judgments, and increases the delay and expense to all parties and the court system presented by the legal and factual issues of the case. By contrast, the class action device presents far fewer management difficulties and provides the benefits of a single adjudication, economy of scale, and comprehensive supervision by a single court.

65. **Rule 23(b)(2)**. Plaintiffs also satisfy the requirements for maintaining a class action under Rule 23(b)(2). Seagate has acted or refused to act on grounds that apply generally

to the proposed classes, making final declaratory or injunctive relief appropriate with respect to the proposed classes as a whole.

66. **Rule 23 (c)(4)**. Plaintiffs also satisfy the requirements for maintaining a class action under Rule 23(c)(4). The claims of class members are composed of particular issues that are common to all class members and capable of class wide resolution that will significantly advance the litigation.

CAUSES OF ACTION

FIRST CAUSE OF ACTION
(Negligence – On Behalf of All Classes)

67. Plaintiffs reallege and incorporate by reference all prior allegations as if fully set forth herein.

68. This cause of action is brought on behalf of all classes.

69. The Employees are or were employed by Seagate and were issued a 2015 Form W-2 from Seagate or for whom Seagate had 2015 Form W-2 data. As a condition of their employment, the Employees were obligated to provide Seagate with certain PII, including their names, addresses, and Social Security numbers. In addition, the Employees provided Seagate with PII of other individuals, such as their spouses and children. Such information was provided, *inter alia*, as information concerning beneficiaries for retirement plans, health insurance coverage or other insurance plans.

70. Seagate had 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. Seagate had a duty to Plaintiffs and each class member to exercise reasonable care in holding, safeguarding and protecting that information. Plaintiffs and the class members were the

foreseeable victims of any inadequate safety and security practices. Plaintiffs and the other class members had no ability to protect their data that was in Seagate's possession.

71. Seagate's duty to the Plaintiffs and other class members included, *inter alia*, establishing processes and procedures to protect the PII from wrongful disclosure and training employees who had access to the PII as to those processes and procedures. Seagate is a significant player in the technology industry, and Seagate, its officers, directors and management are all well aware of the risks associated with the wrongful disclosure of PII and the threats to PII posed by hackers, scammers, and other cybercriminals.

72. In addition, Seagate had a duty to timely and adequately disclose to Plaintiffs and the other class members that their PII had been compromised. Such timely disclosure was necessary to allow Plaintiffs and the other class members to (i) purchase identity protection services; (ii) monitor their bank accounts, credit cards and other financial accounts; and (iii) take other steps to protect against identity theft and the fraudulent use of their PII by third parties.

73. Seagate admitted that Plaintiffs' and the other class members' PII was wrongfully disclosed as a result of the Data Breach. Seagate further admitted that the Data Breach was the result of Seagate's "human error and lack of vigilance, and [that it] could have been protected."

74. As a result of Seagate's negligence, Plaintiffs and the class members have suffered and will continue to suffer damages and injury including, but not necessarily limited to: a) out-of-pocket costs associated with addressing false tax returns filed with the IRS and state tax agencies; b) increased future out of pocket costs in connection with preparing and filing tax returns; c) out-of-pocket costs associated with procuring identity protection and restoration

services; d) in the event of future identity theft, out-of-pocket costs associated with repairing credit, reversing fraudulent charges, and other harms; and e) lost productivity and enjoyment as a result of time spent monitoring, addressing and correcting future consequences of the Data Breach.

75. Seagate breached its duty to Plaintiffs and the class members by failing to maintain proper security measures, policies and procedures, and training. Seagate failed timely to notify Plaintiffs and the class members of the Data Breach. Plaintiffs and the class members have been harmed as a direct and proximate result of Seagate's negligence. Plaintiffs and the class members will continue to be harmed as a direct and proximate result of Seagate's negligence.

76. Plaintiffs and the class members are entitled to money damages for all out-of-pocket costs caused by Seagate's negligence. Plaintiffs also seek reasonable attorneys' fees and costs under the applicable law, including Federal Rule of Civil Procedure 23 and California Code of Civil Procedure § 1021.5.

SECOND CAUSE OF ACTION
(Violation of Unfair Competition Law
California Business and Professional Code Section 17200, *et seq.* – On Behalf of All Classes)

77. Plaintiffs reallege and incorporate by reference all prior allegations as if fully set forth herein.

78. This cause of action is brought on behalf of all classes.

79. Seagate engaged in unfair and unlawful business practices in violation of the Unfair Competition Law, Cal. Bus. & Prof. Code § 17200, *et seq.* ("UCL"). Seagate's acts, omissions and conduct constitute unfair and unlawful business practices under the UCL.

80. Seagate's practices were unlawful and in violation of Civil Code section 1798.81.5 because Seagate failed to take reasonable measures in protecting Plaintiffs' and the class members' PII.

81. Seagate's practices were also unlawful and in violation of Civil Code section 1798.82 because Seagate's notice to Plaintiffs and the class members concerning the Data Breach, as required by the statute, failed to fully disclose the extent of the Data Breach.

82. Seagate's acts, omissions, and conduct also constitute "unfair" business acts or practices because they offend public policy and constitute immoral, unethical, and unscrupulous activities that caused substantial injury, including to Plaintiffs and class members. The gravity of harm resulting from Seagate's conduct outweighs any potential benefits attributable to the conduct and there were reasonably available alternatives to further Seagate's legitimate business interests. Seagate's conduct also undermines public policy as reflected in statutes such as the Information Practices Act of 1977, Cal. Civ. Code § 1798, *et seq*., and the California Customer Records Act, which were enacted to protect individuals' personal data and ensure that entities who solicit or are entrusted with personal data use reasonable security measures

83. Seagate had exclusive knowledge about the extent of the Data Breach, including during the days and weeks following the Data Breach.

84. But for Seagate's misrepresentations and omissions, Plaintiffs and the class members would not have provided the PII that they provided to Seagate or would have insisted that their PII be more securely protected and removed from Seagate's systems promptly after their employment ended. They also would have taken additional steps to protect their identities and to protect themselves from the sort of harm that could flow from Seagate's lax security measures. But for Seagate's misrepresentations and omissions, Plaintiffs and the class members

would not be experiencing identity theft, identity fraud, and/or the increased risk of harm they are now facing, as a result of the Data Breach. But for the fact that Seagate sat on information regarding the Data Breach, rather than immediately disclosing it, Plaintiffs and the class members would have taken more immediate steps to protect their identities and they would have been able to minimize the harm they have suffered as a result of the Data Breach.

85. As a direct and proximate result of Seagate's unlawful and unfair business practices as alleged herein, Plaintiffs and the class members have suffered injury in fact. Plaintiffs and the classes have been injured in that their personal and financial PII has been compromised, subject to identity theft, identity fraud, and/or is at risk for future identity theft and fraudulent activity on their financial accounts. Class members have also lost money and property that would not have been lost but for Seagate's unlawful and unfair conduct.

86. As a direct and proximate result of Seagate's unlawful and unfair business practices as alleged herein, Plaintiffs and class members already suffer from identity theft, identity and financial fraud, and/or a continuing increased risk of identity theft and financial and medical fraud due to the compromise, publication, and/or unauthorized use of their financial PII. Plaintiffs and the class members have also been injured by, among other things: (1) the loss of the opportunity to control how their PII is used; (2) the diminution in the value and/or use of their PII entrusted to Seagate for the purpose of deriving employment from Seagate and with the expectation that Seagate would safeguard their PII against theft and not allow access and misuse of their PII by others; (3) the compromise, publication, and/or theft of their PII; (4) out-of-pocket costs associated with the prevention, detection, and recovery from identity theft and/or unauthorized use of financial and medical accounts; (5) lost opportunity costs associated with effort expended and the loss of productivity from addressing and attempting to mitigate the

actual and future consequences of the breach, including but not limited to efforts spent researching how to prevent, detect, contest and recover from identity and health care/medical data misuse; (6) costs associated with the ability to use credit and assets frozen or flagged due to credit misuse, including complete credit denial and/or increased costs to use credit, credit scores, credit reports and assets; (7) unauthorized use of compromised PII to open new financial and/or health care or medical accounts; (8) tax fraud and/or other unauthorized charges to financial, health care or medical accounts and associated lack of access to funds while proper information is confirmed and corrected; (9) the continued risk to their PII and the PII of their family members and designated beneficiaries of employment-related benefits through Seagate, which remain in Seagate's possession and are subject to further breaches so long as Seagate fails to undertake appropriate and adequate measures to protect the PII in its possession; and (10) future costs in terms of time, effort and money that will be expended to prevent, detect, contest, and repair the impact of the PII compromised as a result of the Data Breach for the remainder of the Plaintiffs' and the class members' lives and the lives of their families and their designated beneficiaries of employment-related benefits through Seagate.

87. As a result of Seagate's violations of the UCL, Plaintiffs and the class members are entitled to injunctive relief, including, but not limited to an order that Seagate: (1) engage third party security auditors/penetration testers as well as internal security personnel to conduct testing consistent with prudent industry practices, including simulated attacks, penetration tests, and audits on Seagate's systems on a periodic basis; (2) engage third party security auditors and internal personnel to run automated security monitoring consistent with prudent industry practices; (3) audit, test, and train its security personnel regarding any new or modified procedures; (4) purge, delete and destroy, in a secure manner, employee data not necessary for

its business operations; (5) conduct regular database scanning and security checks consistent with prudent industry practices; (6) periodically conduct internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach consistent with prudent industry practices; (7) receive periodic compliance audits by a third party regarding the security of the computer systems Seagate uses to store the PII of its current and former employees; (8) meaningfully educate its current and former employees about the threats they face as a result of the loss of their PII to third parties, as well as the steps they must take to protect themselves; and (9) provide ongoing identity theft protection, monitoring, and recovery services to Plaintiffs and class members, as well as to their dependents and designated beneficiaries of employment-related benefits through Seagate.

88. Because of Seagate's unlawful and unfair business practices, Plaintiffs and the class members are entitled to relief, including attorneys' fees and costs, restitution, declaratory and injunctive relief. Plaintiffs also seek reasonable attorneys' fees and costs under applicable law including Federal Rule of Civil Procedure 23 and California Code of Civil Procedure § 1021.5.

THIRD CAUSE OF ACTION
(Declaratory Judgment – On Behalf of All Classes)

89. Plaintiffs reallege and incorporate by reference all prior allegations as if fully set forth herein.

90. This cause of action is brought on behalf of all the classes.

91. As set forth above, Plaintiffs and the class members have valid claims against Seagate for negligence and violations of the UCL. An actual controversy has arisen in the wake

of Seagate's Data Breach regarding Seagate's current obligations to provide reasonable data security measures to protect the PII of Plaintiffs and the class members.

92. Plaintiffs thus seek a declaration that to comply with its existing obligations, Seagate must implement specific additional, prudent industry security practices, as outlined below, to provide reasonable protection and security to the PII of Plaintiffs and the class members. Specifically, Plaintiffs and the class members seek a declaration that (a) Seagate's existing security measures do not comply with its obligations, and (b) that to comply with its obligations, Seagate must implement and maintain reasonable security measures on behalf of Plaintiffs and the Nationwide Class, including, but not limited to: (1) engaging third party security auditors/penetration testers as well as internal security personnel to conduct testing consistent with prudent industry practices, including simulated attacks, penetration tests, and audits on Seagate's systems on a periodic basis; (2) engaging third party security auditors and internal personnel to run automated security monitoring consistent with prudent industry practices; (3) auditing, testing, and training its security personnel regarding any new or modified procedures; (4) purging, deleting and destroying, in a secure manner, employee data not necessary for its business operations; (5) conducting regular database scanning and security checks consistent with prudent industry practices; (6) periodically conducting internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach consistent with prudent industry practices; (7) receiving periodic compliance audits by a third party regarding the security of the computer systems Seagate uses to store the personal information of its current and former employees; (8) meaningfully educating its current and former employees about the threats they face as a result of the loss of their PII to third parties, as well as the steps they must take to protect themselves;

and (9) providing ongoing identity theft protection, monitoring, and recovery services to Plaintiffs and class members, as well as to their dependents and designated beneficiaries of employment-related benefits through Seagate.

93. Each Plaintiff and class member is entitled to a declaration of rights providing that Seagate is obligated, pursuant to terms established by the Court, to reimburse said individuals for any and all future harm caused by the Data Breach.

FOURTH CAUSE OF ACTION
(Breach of Implied Contract – On Behalf of the Employee Class)

94. Plaintiffs re-allege and incorporate by reference all prior allegations as if fully set forth herein.

95. Seagate Employees provided their PII in connection with their employment with Seagate in order to verify their identity, receive compensation and in order for Seagate to have complete employee records for tax purposes, amongst other things.

96. Plaintiffs Everett Castillo, Nicholas Dattoma, Freda Lang, Wendy Tran and Steven Wilk and the Employee class members provided various forms of PII to Seagate as a condition precedent to their employment with Seagate, or in connection with employer sponsored benefits.

97. Understanding the sensitive nature of PII, Seagate implicitly promised Plaintiffs Everett Castillo, Nicholas Dattoma, Freda Lang, Wendy Tran and Steven Wilk and the Employee Class members that it would take adequate measures to protect their PII.

98. Indeed, a material term of this contract is a covenant by Seagate that it will take reasonable efforts to safeguard Employees' PII.

99. Seagate's current and former employees, including Plaintiffs Everett Castillo, Nicholas Dattoma, Freda Lang, Wendy Tran and Steven Wilk and the Employee class members, relied upon this covenant and would not have disclosed their PII without assurances that it would be properly safeguarded. Moreover, the covenant to adequately safeguard the PII of Plaintiffs Everett Castillo, Nicholas Dattoma, Freda Lang, Wendy Tran and Steven Wilk and Employee class members is an implied term, to the extent it is not an express term.

100. Plaintiffs Everett Castillo, Nicholas Dattoma, Freda Lang, Wendy Tran and Steven Wilk and the Employee class members fulfilled their obligations under the contract by providing their PII to Seagate.

101. Seagate however, failed to safeguard and protect the PII of Plaintiffs Everett Castillo, Nicholas Dattoma, Freda Lang, Wendy Tran and Steven Wilk and the Employee class members. Seagate's breach of its obligations under the contract between the parties directly caused Plaintiffs Everett Castillo, Nicholas Dattoma, Freda Lang, Wendy Tran and Steven Wilk and Employee class members to suffer injuries.

102. Plaintiffs Everett Castillo, Nicholas Dattoma, Freda Lang, Wendy Tran and Steven Wilk, on behalf of themselves and the Employee class members, respectfully request this Court award all relevant damages for Seagate's breach of contract.

PRAYER FOR RELIEF

Plaintiffs, on behalf of themselves and on behalf of the proposed classes, request that the Court:

a. Certify this case as a class action, appoint Plaintiffs as class representatives and appoint Plaintiffs' counsel to represent the classes;

b. Find that Seagate breached its duty to safeguard and protect Plaintiffs' and the class members' PII which was compromised in the Data Breach;

c. Award Plaintiffs and Class members appropriate relief, including actual damages, punitive damages, and statutory damages;

d. Award equitable, injunctive, declaratory relief as appropriate;

e. Award all costs, including experts' fees and attorneys' fees, and the costs of prosecuting this action;

f. Award pre-judgment and post-judgment interest as prescribed by law; and

g. Grant additional legal or equitable relief as the Court may find just and proper.

DEMAND FOR JURY TRIAL

Plaintiffs hereby demand a trial by jury on all issues so triable.

Dated: October 18, 2016

Respectfully submitted,

GLANCY PRONGAY & MURRAY LLP

By: *s/ Mark S. Greenstone*

Marc L. Godino
Mark S. Greenstone
1925 Century Park East, Suite 2100
Los Angeles, CA 90067
Telephone: (310) 201-9150
Facsimile: (310) 201-9160
E-mail: info@glancylaw.com

BRAGAR EAGEL & SQUIRE, P.C.
David J. Stone (*Pro Hac Vice*)
Jeffrey H. Squire (*Pro Hac Vice*)
Lawrence P. Eagel (*Pro Hac Vice*)
885 Third Avenue, Suite 3040
New York, NY 10022
Telephone: (212) 308-5858
Facsimile: (212) 486-0462
E-mail: stone@bespc.com
squire@bespc.com
eagel@bespc.com

Counsel for Plaintiffs Everett Castillo, Linda Castillo, Wendy Tran and the Class

Eric A. Grover (SBN 136080)
KELLER GROVER LLP
1965 Market Street
San Francisco, California 94103
Telephone: (415) 543-1305
Facsimile: (415) 543-7861
eagrover@kellergrover.com

Jeremiah Frei-Pearson (*Pro Hac Vice* forthcoming)
FINKELSTEIN, BLANKINSHIP, FREI-PEARSON & GARBER, LLP
445 Hamilton Ave, Suite 605 White Plains, New York 10601
Telephone: (914) 298-3281
Fax: (914) 908-6709
jfrei-pearson@fbfglaw.com

Counsel for Plaintiff Nicholas Dattoma, Freda Lang, Steven Wilk and the Class

PROOF OF SERVICE VIA ELECTRONIC POSTING PURSUANT TO NORTHERN DISTRICT OF CALIFORNIA LOCAL RULES AND LOCAL CIVIL RULE 5-1

I, the undersigned, say:

I am a citizen of the United States and am over the age of 18 and not a party to the within action. My business address is 1925 Century Park East, Suite 2100, Los Angeles, California 90067.

On October 18, 2016, I served the following document:

FIRST AMENDED CONSOLIDATED CLASS ACTION COMPLAINT

By posting the document to the ECF Website of the United States District Court for the Northern District of California, for receipt electronically by the parties as listed on the attached Court's ECF Service List.

And on any non-ECF registered parties:

By U.S. Mail: By placing true and correct copies thereof in individual sealed envelope: with postage thereon fully prepaid, which I deposited with my employer for collection and mailing by the United States Postal Service. I am readily familiar with my employer's practice for the collection and processing of correspondence or mailing with the United States Postal Service. In the ordinary course of business, this correspondence would be deposited by my employer with the United States Postal Service that same day.

I certify under penalty of perjury under the laws of the United States of America that the foregoing is true and correct. Executed on October 18, 2016, at Los Angeles, California.

s/ Mark S. Greenstone
Mark S. Greenstone

Mailing Information for a Case 3:16-cv-01958-RS Castillo et al v. Seagate Technology, LLC

Electronic Mail Notice List

The following are those who are currently on the list to receive e-mail notices for this case.

- **Tiffany Cheung**
  tcheung@mofo.com,lucia-sario-5135@ecf.pacerpro.com,tiffany-cheung-0452@ecf.pacerpro.com,lsario@mofo.com,lisaflores@mofo.com
- **Lawrence Paul Eagel**
  eagel@bespc.com
- **Jeremiah Frei-Pearson**
  jfrei-pearson@fbfglaw.com
- **Todd S. Garber**
  tgarber@fbfglaw.com
- **Lionel Z. Glancy**
  info@glancylaw.com,lglancy@glancylaw.com
- **Marc Lawrence Godino**
  mgodino@glancylaw.com,info@glancylaw.com
- **Mark Samuel Greenstone**
  mgreenstone@glancylaw.com,info@glancylaw.com
- **Eric A. Grover**
  eagrover@kellergrover.com,eacevedo@kellergrover.com,Reception@kellergrover.com,sholloway@kellergrover.com,rjung@kellergrover.com,rspencer@kellergrover.com
- **Alexandra Eve Laks**
  alaks@mofo.com,gina-gerrish-5550@ecf.pacerpro.com,ggerrish@mofo.com,alexandra-laks-0787@ecf.pacerpro.com
- **David Frank McDowell**
  dmcdowell@mofo.com,docket-la@mofo.com,david-mcdowell-0950@ecf.pacerpro.com,etovar@mofo.com,elizabeth-tovar-4810@ecf.pacerpro.com
- **Jeffrey H. Squire**
  squire@bespc.com
- **David Jay Stone**
  stone@bespc.com

Manual Notice List

The following is the list of attorneys who are **not** on the list to receive e-mail notices for this case (who therefore require manual noticing). You may wish to use your mouse to select and copy this list into your word processing program in order to create notices or labels for these recipients.

- (No manual recipients)