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 AND WENDY TRAN, INDIVIDUALLY AND ON BEHALF OF ALL OTHERS SIMILARLY SITUATED, Plaintiffs, v. SEAGATE TECHNOLOGY, LLC, Defendant.	Case No.: CLASS ACTION **CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

Everett Castillo, Linda Castillo and Wendy Tran ("Plaintiffs"), individually and on behalf of all others similarly situated, file this 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. On or about March 1, 2016, a Seagate employee responded to an Internet "phishing" 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 names, addresses, salaries and, most importantly, Social Security numbers.

2. Almost immediately, the cybercriminals exploited Seagate's wrongful actions and filed fraudulent federal and state tax returns in the names of the 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. In order for the cybercriminals to have obtained Employees' spouse's Social Security numbers, Seagate would have had to have disclosed more than just the Form W-2 data for Employees. Seagate would have to have disclosed additional information, such as retirement fund or insurance beneficiary information that contained the PII of third parties ("Third-Party Victims").

[1] As used herein, "Seagate" includes any Seagate affiliates and subsidiaries for which Seagate processed and/or stored the Employees' 2015 Forms W-2 or information included in the Employees' 2015 Forms W-2. 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.

3. No one can know what else the cybercriminals will do with the Employees' and Third-Party Victims' PII. However, the Employees and Third-Party Victims are now, and for the rest of their lives will be, at a heightened risk of identity theft. 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.

JURISDICTION AND VENUE

4. This Court has jurisdiction over the claims in this action pursuant to 28 U.S.C. § 1332(d) because the amount in controversy exceeds $5 million, exclusive of interest and costs, and members of the proposed classes are citizens of different states than Defendant Seagate.

5. 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.

6. 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

7. 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.

8. 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.

9. 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.

10. 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

11. Seagate has represented that on or about March 1, 2016, 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.

12. 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 Seagate disclosed in the Data Breach more information than just Form W-2 data.

13. 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.

14. 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.

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

16. The cybercriminals obtained the Employees' and Third-Party Victims' information through a typical "phishing" scam. Seagate has admitted that the cybercriminals

sent bogus emails to human resources and payroll employees at Seagate and asked for copies of all of its 2015 Forms W-2 data. Due to the lack of training, procedures and controls in place at Seagate, at least one employee complied with the cybercriminals' request and forwarded copies of all of the Employees' Forms W-2 data to the cybercriminals.

17. Seagate has not made any comments about Third-Party Victims' PII.

18. Following discovery of the Data Breach, Seagate focused on protecting itself rather than the Employees who had been victimized. Current employees received an email from the company three days later on or about March 4, 2016, informing them that their personal information had been disclosed. Former employees did not receive notification from Seagate until much later. Seagate sent former employees a letter dated March 9, 2016 – which was often not received until Mach 15, 2006, informing them of the scam. Many of the former employees learned of the Data Breach through alternative sources. By the time current and former employees received notice of the Data Breach, many were already the victims of identity theft.

19. Seagate was not without warning of the phishing scam. Prior to the attack, 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.[2]

20. Seagate's negligence in safeguarding the Employees' and Third-Party Victims' PII is exacerbated by the fact that the company touts the high level of security and encryption

[2] "Phishers Spoof CEO, Request W2 Forms," Krebsonsecurity.com. http://bit.ly/25oAc2c.

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[3]

21. 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 Have Been Damaged

22. The Employees were obligated to provide Seagate with sensitive personal information, including their Social Security numbers. In addition, in order to obtain certain benefits, such as retirement plan 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.

23. 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 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

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

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.

24. Plaintiff Tran is an Employee whose 2015 Form W-2 data was disclosed by Seagate. 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. 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 will incur additional costs with respect to the accountant that she would not have had to pay, but for the Data Breach.

25. 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.

26. 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. 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.

27. Plaintiff Everett Castillo is an Employee whose 2015 Form W-2 data was disclosed by Seagate. Plaintiff Linda Castillo is Mr. Castillo's wife. 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, had not worked for Seagate or one of its affiliates and did not receive a Form W-2 from Seagate.

28. 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 not 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 Ms. Castillo (or Mr. Castillo) for the time spent addressing the fraudulent tax return filed on their behalf.

29. 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. Such harm includes, but is not necessarily limited to,

Employees who learned that cybercriminals have obtained fraudulent lines of credit using their Social Security numbers.

Seagate's Inadequate Response to Protect the Employees

30. 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.

31. 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 at all 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.

32. 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." [4] 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).[5]

Class Action Allegations

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

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

c. **Nationwide Third-Party Class**: All non-current or 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.

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

34. **Numerosity**. The proposed class and sub-classes contain thousands of individuals dispersed throughout the United States and throughout individual states. Joinder of all members is impracticable. Class members can be identified through Seagate's records.

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

35. **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 PII of the Nationwide Third-Party Class and the California Third-Party Class.

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

e. Whether class members are entitled to actual damages and/or statutory damages; and

f. Whether class members are entitled to injunctive relief.

36. **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.

37. **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.

38. **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.

39. **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.

40. **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)

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

42. This cause of action is brought on behalf of all of the sub-classes.

43. 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.

44. 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.

45. 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.

46. 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.

47. 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."

48. 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.

49. 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.

50. 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.*)

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

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

53. Seagate engaged in unfair, unlawful and fraudulent 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, unlawful and fraudulent business practices under the UCL.

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

55. Seagate's practices were also unlawful and in violation of Civil Code section 1798.82 because Seagate unreasonably delayed informing Plaintiffs and the class members about the breach of security after Seagate knew the breach occurred.

56. 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

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

58. 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.

59. As a direct and proximate result of Seagate's unlawful, unfair, and fraudulent business practices as alleged herein, Plaintiffs and members of the classes 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.

60. As a direct and proximate result of Seagate's unlawful, unfair, and fraudulent 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.

61. 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.

62. Because of Seagate's unlawful, unfair, and fraudulent business practices, Plaintiffs and the class members are entitled to relief, including attorneys' fees and costs, restitution, declaratory relief, and a permanent injunction enjoining Seagate from its unlawful

and unfair practices. 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)

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

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

65. 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.

66. 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.

67. 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.

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 demands a trial by jury on all issues so triable.

Dated: April 14, 2016

Respectfully submitted,

GLANCY PRONGAY & MURRAY LLP

By: *s/ Mark S. Greenstone*

Lionel Z. Glancy
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
Jeffrey H. Squire
Lawrence P. Eagel
885 Third Avenue, Suite 3040
New York, NY 10022
Telephone: (212) 308-5858
Facsimile: (212) 486-0462
E-mail: info@bespc.com

Counsel for Plaintiffs