

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

7 *Counsel for Plaintiffs*
[Additional Counsel Listed On Signature Page]

9 UNITED STATES DISTRICT COURT
10 NORTHERN DISTRICT OF CALIFORNIA

11 EVERETT CASTILLO, LINDA
12 CASTILLO AND WENDY TRAN,
13 INDIVIDUALLY AND ON BEHALF OF
14 ALL OTHERS SIMILARLY SITUATED,

15 Plaintiffs,

16 v.

17 SEAGATE TECHNOLOGY, LLC,

18 Defendant.

Case No.:

CLASS ACTION

CLASS ACTION COMPLAINT

JURY TRIAL DEMANDED

1 3. No one can know what else the cybercriminals will do with the Employees' and
2 Third-Party Victims' PII. However, the Employees and Third-Party Victims are now, and for
3 the rest of their lives will be, at a heightened risk of identity theft. Many Employees and Third-
4 Party Victims have already suffered out-of-pocket costs attempting to rectify fraudulent tax
5 returns and engaging services to monitor and protect their identity and credit. Employees and
6 Third-Party Victims will continue to suffer out-of-pocket costs in the future to protect and, if
7 necessary, repair their credit and identity. By this action, Plaintiffs seek to hold Seagate
8 responsible for the harm caused by its negligence.
9

10 **JURISDICTION AND VENUE**

11 4. This Court has jurisdiction over the claims in this action pursuant to 28 U.S.C. §
12 1332(d) because the amount in controversy exceeds \$5 million, exclusive of interest and costs,
13 and members of the proposed classes are citizens of different states than Defendant Seagate.
14

15 5. This Court has personal jurisdiction over Seagate because Seagate maintains its
16 principal place of business in this District, is registered to conduct business in California, and
17 has sufficient minimum contacts with California.
18

19 6. Venue is proper in this District pursuant to 28 U.S.C. § 1391(b) because Seagate
20 resides in this District and a substantial part of the events or omissions giving rise to Plaintiffs'
21 claims occurred in this District.
22

23 **PARTIES**

24 7. Plaintiff Everett Castillo is a resident of California and an Employee. In 2015,
25 Mr. Castillo was employed by Lyve Minds, Inc. ("Lyve"). Lyve was acquired by Seagate
26 during 2015 and maintained as a Seagate subsidiary. Although Mr. Castillo received his 2015
27
28

1 Form W-2 from Lyve, Seagate had Mr. Castillo's Form W-2 data. Seagate informed Mr.
2 Castillo that Seagate had disclosed his Form W-2 data in the Data Breach.

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

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

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

13 **FACTUAL ALLEGATIONS**

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

20 12. Almost immediately, the cybercriminals began to exploit the Employees' PII by,
21 *inter alia*, filing false federal and state tax returns for some or all of the Employees. In some
22 cases, the cybercriminals filed joint tax returns, on behalf of an Employee and his or her spouse.
23 The false joint tax returns used the Employee's spouse's Social Security number. Form W-2
24
25
26
27
28

1 data does not contain the Social Security number for spouses. The fact that the cybercriminals
2 had obtained the Social Security number for at least some of the Employees' spouses suggests
3 that Seagate disclosed in the Data Breach more information than just Form W-2 data.

4 13. The cybercriminals who obtained the Employees' and Third-Party Victims' PII
5 may continue to exploit the data themselves and/or sell the data in the so-called "dark markets."
6 Having obtained the Employees' and Third-Party Victims' names, addresses and Social
7 Security numbers, cybercriminals can pair the data with other available information to commit a
8 broad range of fraud in an Employee's name, including but not limited to:
9

- 10 a. obtaining employment;
- 11 b. obtaining a loan;
- 12 c. applying for credit cards or spending money;
- 13 d. filing false tax returns;
- 14 e. obtaining medical care;
- 15 f. stealing Social Security and other government benefits; and
- 16 g. applying for a driver's license, birth certificate or other public document.

17
18
19 14. In addition, if an Employee's or Third-Party Victims' Social Security number is
20 used to create a false identification for someone who commits a crime, the Employee or Third-
21 Party Victim may become entangled in the criminal justice system, impairing the Employee's or
22 Third-Party Victim's ability to gain employment or obtain a loan.

23
24 15. For the rest of their lives, Plaintiffs and the class members will bear a heightened
25 risk of all manners of identity theft.

26 16. The cybercriminals obtained the Employees' and Third-Party Victims'
27 information through a typical "phishing" scam. Seagate has admitted that the cybercriminals
28

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

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

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

16 19. Seagate was not without warning of the phishing scam. Prior to the attack,
17 Internet security researcher Brian Krebs warned of this precise scam on his Internet website.
18 Krebs warned that as tax season approached Internet scammers were trying to scam various
19 companies by sending false emails, purportedly from the company's chief executive officer, to
20 individuals in the human resources and accounting departments and asking for copies of Forms
21 W-2 data.²
22

23 20. Seagate's negligence in safeguarding the Employees' and Third-Party Victims'
24 PII is exacerbated by the fact that the company touts the high level of security and encryption
25
26
27

28 _____
² "Phishers Spoof CEO, Request W2 Forms," Krebs on security.com. <http://bit.ly/25oAc2c>.

1 features available with its own products. For example, Seagate’s website describes the security
2 features for its hard drives:

3 Secure your data with Seagate’s portfolio of Self-Encrypting Drives (SED)
4 for enterprise and PCs with options like Seagate Instant Secure Erase (ISE)
5 for painless drive retirement and the world’s only FIPS 140-2 validated hard
6 drive solution. Choose the level of ‘data-at-rest’ security that’s right for you.
7 Seagate Secure™ Technology³

8 21. Seagate conceded its fault in the Data Breach. Seagate’s Chief Financial Officer
9 wrote in a March 4, 2016 email to employees: “This mistake was caused by human error and
10 lack of vigilance, and could have been prevented.”

11 **Seagate’s Current and Former Employees Have Been Damaged**

12 22. The Employees were obligated to provide Seagate with sensitive personal
13 information, including their Social Security numbers. In addition, in order to obtain certain
14 benefits, such as retirement plan or insurance benefits, Employees must provide Seagate with
15 PII for their beneficiaries as well. Seagate had a duty to protect that information against
16 wrongful disclosure to third parties. Seagate failed to comply with its duties to its current and
17 former employees and their beneficiaries by failing to implement policies and procedures to
18 prevent cybercriminals and scammers from obtaining the Employees’ and Third-Party Victims’
19 PII.
20

21 23. As a result of the Data Breach, numerous Employees and Third-Party Victims
22 have already suffered damages. In addition, the disclosure of an individual’s Social Security
23 number puts one at great risk of future fraudulent conduct. By pairing a Social Security number
24 with someone’s name, address and, perhaps, other readily available information, an identity
25 thief can commit a broad range of fraud, including but not limited to a) obtaining
26

27
28 _____
³ <http://www.seagate.com/solutions/security/>

1 unemployment; b) obtaining a loan; c) applying for credit cards or spending money under the
2 victim's name; d) filing false tax returns; e) obtaining medical care; f) stealing Social Security
3 and other government benefits; and g) applying for a driver's license, birth certificate or other
4 public document. Any of these activities can cause significant financial and emotional harm to
5 a victim. Even if the victim applies for and receives a replacement Social Security number, he
6 or she will not be free from risk.

8 24. Plaintiff Tran is an Employee whose 2015 Form W-2 data was disclosed by
9 Seagate. When Ms. Tran learned about the Data Breach, she promptly investigated and learned
10 that both a fraudulent federal tax return and a fraudulent state tax return had been filed on her
11 behalf. Although Ms. Tran usually prepares and files her federal and state tax returns on her
12 own, she retained the services of an accountant to assist with redressing the fraudulent tax
13 returns and filing her 2015 federal and state returns. Ms. Tran will incur additional costs with
14 respect to the accountant that she would not have had to pay, but for the Data Breach.
15

16 25. Ms. Tran has spoken with individuals at the California Franchise Tax Board to
17 determine what she must do to file her state returns going forward, and she has received
18 different advice. One individual told her that she cannot e-file her state taxes for the foreseeable
19 future. Another individual told her that she can e-file, but if she is getting a state tax refund, she
20 must call a certain telephone number to confirm the refund before the state will release it.
21

22 26. Although Seagate offered Ms. Tran (along with other Employees) two years of
23 limited identity theft protection through Experian's ProtectMyID service, Ms. Tran is unable to
24 take advantage of this service. Ms. Tran already has a subscription to ProtectMyID because she
25 was a victim of a prior unrelated data breach. Experian informed Ms. Tran that she cannot
26 create a second subscription. Further, her current ProtectMyID subscription will lapse in a few
27
28

1 months' time – but not until after the deadline for signing up for the Seagate sponsored
2 ProtectMyID service. Ms. Tran is effectively unable to obtain any relief from Seagate.

3 27. Plaintiff Everett Castillo is an Employee whose 2015 Form W-2 data was
4 disclosed by Seagate. Plaintiff Linda Castillo is Mr. Castillo's wife. Soon after learning of the
5 Data Breach, the Castillos investigated whether false tax returns had been filed on their behalf.
6 They learned that a fraudulent joint federal tax return had been filed on their behalf. The
7 fraudulent tax returns contained both Mr. Castillo's Social Security number and Ms. Castillo's
8 Social Security number. Ms. Castillo, however, had not worked for Seagate or one of its
9 affiliates and did not receive a Form W-2 from Seagate.

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

20 29. In addition, Plaintiffs, Employees and Third Party Victims will be at risk of
21 identity theft for the rest of their lives, requiring constant diligence and monitoring. Upon
22 information and belief, other Employees have suffered harm as a result of the Data Breach in
23 addition to fraudulent tax returns. Such harm includes, but is not necessarily limited to,
24
25
26
27
28

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

3 **Seagate's Inadequate Response to Protect the Employees**

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

15 31. The offered ProtectMyID service is inadequate to protect the Employees from
16 the threats they face. It does nothing to protect *against* identity theft. Instead, it only provides a
17 measure of assistance after identity theft has been discovered. For example, ProtectMyID only
18 monitors Employees' *credit reports* – but fraudulent activity, such as the filing of a false tax
19 return, may not appear at all on a credit report. ProtectMyID *does not* provide real time
20 monitoring of Employees' credit cards and bank account statements. Employees must pay extra
21 for that service. Although ProtectMyID offers up to \$1 million of identity theft insurance, the
22 coverage afforded is limited and often duplicative of (or inferior to) basic protections provided
23 by banks and credit card companies.

26 32. Many websites that rank identity protection services are critical of ProtectMyID.
27 NextAdvisor ranks ProtectMyID at the bottom of comparable services, noting that it “lacks in
28

1 protection; only includes Experian credit report monitoring; 7-day trial for \$1 with enrollment;
2 credit score and other credit reports cost extra.”⁴ BestIDtheftCompanys.com ranks
3 ProtectMyID at No 30 with a score of just 4.4 out of 10 (and a “User Score” of just 1.3).⁵

4 **Class Action Allegations**

5 33. Plaintiffs bring these claims pursuant to Federal Rule of Civil Procedure 23 on
6 behalf of classes of similarly situated persons, which they propose to be defined as follows:
7

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

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

13 c. **Nationwide Third-Party Class:** All non-current or former Seagate or Seagate
14 affiliates’ employees whose PII was compromised as a result of the Data Breach, including but
15 not limited to spouses, children or other individuals associated with Employees.
16

17 d. **California Third-Party Class:** All non-current or former Seagate or Seagate
18 affiliates’ employees residing in California whose PII was compromised as a result of the Data
19 Breach, including but not limited to spouses, children or other individuals associated with
20 Employees.
21

22 34. **Numerosity.** The proposed class and sub-classes contain thousands of
23 individuals dispersed throughout the United States and throughout individual states. Joinder of
24 all members is impracticable. Class members can be identified through Seagate’s records.
25
26

27
28 ⁴ “Identity Theft Protection Reviews & Prices,” NextAdvisor.com. <http://bit.ly/1UCnsRP>.

⁵ “Experian ProtectMyID,” bestidtesftcompanys.com. <http://bit.ly/1Rh1YGy>.

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

4 a. Whether and to what extent Seagate had a duty to protect the class members' PII;
5 b. Whether Seagate breached its duty to protect the class members' PII;
6 c. Whether Seagate disclosed PII of the Nationwide Third-Party Class and the
7 California Third-Party Class.

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

10 e. Whether class members are entitled to actual damages and/or statutory damages;
11 and
12 f. Whether class members are entitled to injunctive relief.

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

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

21 38. **Rule 23(b)(3).** In addition to satisfying the prerequisites of Rule 23(a), Plaintiffs
22 satisfy the requirements for maintaining a class action under Rule 23(b)(3). Common questions
23 of law and fact predominate over any questions affecting only individual class members and a
24

1 names, addresses, and Social Security numbers. In addition, the Employees provided Seagate
2 with PII of other individuals, such as their spouses and children. Such information was
3 provided, *inter alia*, as information concerning beneficiaries for retirement plans, health
4 insurance coverage or other insurance plans.

5
6 44. Seagate had full knowledge of the sensitivity of the PII and the types of harm
7 that Plaintiffs and class members could and would suffer if the PII were wrongfully disclosed.
8 Seagate had a duty to Plaintiffs and each class member to exercise reasonable care in holding,
9 safeguarding and protecting that information. Plaintiffs and the class members were the
10 foreseeable victims of any inadequate safety and security practices. Plaintiffs and the other
11 class members had no ability to protect their data that was in Seagate's possession.

12
13 45. Seagate's duty to the Plaintiffs and other class members included, *inter alia*,
14 establishing processes and procedures to protect the PII from wrongful disclosure and training
15 employees who had access to the PII as to those processes and procedures. Seagate is a
16 significant player in the technology industry, and Seagate, its officers, directors and
17 management are all well aware of the risks associated with the wrongful disclosure of PII and
18 the threats to PII posed by hackers, scammers, and other cybercriminals.

19
20 46. In addition, Seagate had a duty to timely and adequately disclose to Plaintiffs and
21 the other class members that their PII had been compromised. Such timely disclosure was
22 necessary to allow Plaintiffs and the other class members to (i) purchase identity protection
23 services; (ii) monitor their bank accounts, credit cards and other financial accounts; and (iii)
24 take other steps to protect against identity theft and the fraudulent use of their PII by third
25 parties.
26
27
28

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

5 48. As a result of Seagate's negligence, Plaintiffs and the class members have
6 suffered and will continue to suffer damages and injury including, but not necessarily limited to:
7 a) out-of-pocket costs associated with addressing false tax returns filed with the IRS and state
8 tax agencies; b) increased future out of pocket costs in connection with preparing and filing tax
9 returns; c) out-of-pocket costs associated with procuring identity protection and restoration
10 services; d) in the event of future identity theft, out-of-pocket costs associated with repairing
11 credit, reversing fraudulent charges, and other harms; and e) lost productivity and enjoyment as
12 a result of time spent monitoring, addressing and correcting future consequences of the Data
13 Breach.

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

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

SECOND CAUSE OF ACTION
(Violation of Unfair Competition Law

California Business and Professional Code Section 17200, *et seq.*)

1
2
3 51. Plaintiffs reallege and incorporate by reference all prior allegations as if fully set
4 forth herein.

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

6
7 53. Seagate engaged in unfair, unlawful and fraudulent business practices in
8 violation of the Unfair Competition Law, Cal. Bus. & Prof. Code § 17200, *et seq.* (“UCL”).
9 Seagate’s acts, omissions and conduct constitute unfair, unlawful and fraudulent business
10 practices under the UCL.

11 54. Seagate’s practices were unlawful and in violation of Civil Code section
12 1798.81.5(b) because Seagate failed to take reasonable measures in protecting Plaintiffs’ and
13 the class members’ PII.
14

15 55. Seagate’s practices were also unlawful and in violation of Civil Code section
16 1798.82 because Seagate unreasonably delayed informing Plaintiffs and the class members
17 about the breach of security after Seagate knew the breach occurred.
18

19 56. Seagate’s acts, omissions, and conduct also constitute “unfair” business acts or
20 practices because they offend public policy and constitute immoral, unethical, and unscrupulous
21 activities that caused substantial injury, including to Plaintiffs and class members. The gravity
22 of harm resulting from Seagate’s conduct outweighs any potential benefits attributable to the
23 conduct and there were reasonably available alternatives to further Seagate’s legitimate business
24 interests. Seagate’s conduct also undermines public policy as reflected in statutes such as the
25 Information Practices Act of 1977, Cal. Civ. Code § 1798, *et seq.*, and the California Customer
26 Records Act, which were enacted to protect individuals’ personal data and ensure that entities
27 who solicit or are entrusted with personal data use reasonable security measures
28

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

3 58. But for Seagate's misrepresentations and omissions, Plaintiffs and the class
4 members would not have provided the PII that they provided to Seagate or would have insisted
5 that their PII be more securely protected and removed from Seagate's systems promptly after
6 their employment ended. They also would have taken additional steps to protect their identities
7 and to protect themselves from the sort of harm that could flow from Seagate's lax security
8 measures. But for Seagate's misrepresentations and omissions, Plaintiffs and the class members
9 would not be experiencing identity theft, identity fraud, and/or the increased risk of harm they
10 are now facing, as a result of the Data Breach. But for the fact that Seagate sat on information
11 regarding the Data Breach, rather than immediately disclosing it, Plaintiffs and the class
12 members would have taken more immediate steps to protect their identities and they would have
13 been able to minimize the harm they have suffered as a result of the Data Breach.
14

15 59. As a direct and proximate result of Seagate's unlawful, unfair, and fraudulent
16 business practices as alleged herein, Plaintiffs and members of the classes have suffered injury
17 in fact. Plaintiffs and the classes have been injured in that their personal and financial PII has
18 been compromised, subject to identity theft, identity fraud, and/or is at risk for future identity
19 theft and fraudulent activity on their financial accounts. Class members have also lost money
20 and property that would not have been lost but for Seagate's unlawful and unfair conduct.
21

22 60. As a direct and proximate result of Seagate's unlawful, unfair, and fraudulent
23 business practices as alleged herein, Plaintiffs and class members already suffer from identity
24 theft, identity and financial fraud, and/or a continuing increased risk of identity theft and
25 financial and medical fraud due to the compromise, publication, and/or unauthorized use of
26
27
28

1 their financial PII. Plaintiffs and the class members have also been injured by, among other
2 things: (1) the loss of the opportunity to control how their PII is used; (2) the diminution in the
3 value and/or use of their PII entrusted to Seagate for the purpose of deriving employment from
4 Seagate and with the expectation that Seagate would safeguard their PII against theft and not
5 allow access and misuse of their PII by others; (3) the compromise, publication, and/or theft of
6 their PII; (4) out-of-pocket costs associated with the prevention, detection, and recovery from
7 identity theft and/or unauthorized use of financial and medical accounts; (5) lost opportunity
8 costs associated with effort expended and the loss of productivity from addressing and
9 attempting to mitigate the actual and future consequences of the breach, including but not
10 limited to efforts spent researching how to prevent, detect, contest and recover from identity and
11 health care/medical data misuse; (6) costs associated with the ability to use credit and assets
12 frozen or flagged due to credit misuse, including complete credit denial and/or increased costs
13 to use credit, credit scores, credit reports and assets; (7) unauthorized use of compromised PII to
14 open new financial and/or health care or medical accounts; (8) tax fraud and/or other
15 unauthorized charges to financial, health care or medical accounts and associated lack of access
16 to funds while proper information is confirmed and corrected; (9) the continued risk to their PII
17 and the PII of their family members and designated beneficiaries of employment-related
18 benefits through Seagate, which remain in Seagate's possession and are subject to further
19 breaches so long as Seagate fails to undertake appropriate and adequate measures to protect the
20 PII in its possession; and (10) future costs in terms of time, effort and money that will be
21 expended to prevent, detect, contest, and repair the impact of the PII compromised as a result of
22 the Data Breach for the remainder of the Plaintiffs' and the class members' lives and the lives of
23
24
25
26
27
28

1 their families and their designated beneficiaries of employment-related benefits through
2 Seagate.

3 61. As a result of Seagate's violations of the UCL, Plaintiffs and the class members
4 are entitled to injunctive relief, including, but not limited to an order that Seagate: (1) engage
5 third party security auditors/penetration testers as well as internal security personnel to conduct
6 testing consistent with prudent industry practices, including simulated attacks, penetration tests,
7 and audits on Seagate's systems on a periodic basis; (2) engage third party security auditors and
8 internal personnel to run automated security monitoring consistent with prudent industry
9 practices; (3) audit, test, and train its security personnel regarding any new or modified
10 procedures; (4) purge, delete and destroy, in a secure manner, employee data not necessary for
11 its business operations; (5) conduct regular database scanning and security checks consistent
12 with prudent industry practices; (6) periodically conduct internal training and education to
13 inform internal security personnel how to identify and contain a breach when it occurs and what
14 to do in response to a breach consistent with prudent industry practices; (7) receive periodic
15 compliance audits by a third party regarding the security of the computer systems Seagate uses
16 to store the PII of its current and former employees; (8) meaningfully educate its current and
17 former employees about the threats they face as a result of the loss of their PII to third parties,
18 as well as the steps they must take to protect themselves; and (9) provide ongoing identity theft
19 protection, monitoring, and recovery services to Plaintiffs and class members, as well as to their
20 dependents and designated beneficiaries of employment-related benefits through Seagate.
21
22
23
24

25 62. Because of Seagate's unlawful, unfair, and fraudulent business practices,
26 Plaintiffs and the class members are entitled to relief, including attorneys' fees and costs,
27 restitution, declaratory relief, and a permanent injunction enjoining Seagate from its unlawful
28

1 and unfair practices. Plaintiffs also seek reasonable attorneys’ fees and costs under applicable
2 law including Federal Rule of Civil Procedure 23 and California Code of Civil Procedure §
3 1021.5

4 **THIRD CAUSE OF ACTION**
5 (Declaratory Judgment)

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

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

9
10 65. As set forth above, Plaintiffs and the class members have valid claims against
11 Seagate for negligence and violations of the UCL. An actual controversy has arisen in the wake
12 of Seagate’s Data Breach regarding Seagate’s current obligations to provide reasonable data
13 security measures to protect the PII of Plaintiffs and the class members.

14 66. Plaintiffs thus seek a declaration that to comply with its existing obligations,
15 Seagate must implement specific additional, prudent industry security practices, as outlined
16 below, to provide reasonable protection and security to the PII of Plaintiffs and the class
17 members. Specifically, Plaintiffs and the class members seek a declaration that (a) Seagate’s
18 existing security measures do not comply with its obligations, and (b) that to comply with its
19 obligations, Seagate must implement and maintain reasonable security measures on behalf of
20 Plaintiffs and the Nationwide Class, including, but not limited to: (1) engaging third party
21 security auditors/penetration testers as well as internal security personnel to conduct testing
22 consistent with prudent industry practices, including simulated attacks, penetration tests, and
23 audits on Seagate’s systems on a periodic basis; (2) engaging third party security auditors and
24 internal personnel to run automated security monitoring consistent with prudent industry
25 practices; (3) auditing, testing, and training its security personnel regarding any new or
26
27
28

- 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