Daniel S. Robinson (SBN 244245)
Wesley K. Polischuk (SBN 254121)
Michael W. Olson (SBN 312857)
ROBINSON CALCAGNIE, INC.
19 Corporate Plaza Drive
Newport Beach, CA 92660
(949) 720-1288; Fax (949) 720-1292
drobinson@robinsonfirm.com
wpolischuk@robinsonfirm.com
molson@robinsonfirm.com

M. Anderson Berry (SBN 262879)
Leslie Guillon (SBN 222400)
CLAYEO C. ARNOLD, A PROFESSIONAL LAW CORPORATION
865 Howe Avenue
Sacramento, CA 95825
Telephone: (916) 777-7777
Facsimile: (916) 924-1829
aberry@justice4you.com
lguillon@justice4you.com

Jean Martin (*Pro Hac Vice Forthcoming*)
Ryan J. McGee (*Pro Hac Vice Forthcoming*)
MORGAN & MORGAN COMPLEX LITIGATION GROUP
201 N. Franklin St., 7th Floor
Tampa, FL 33602
Telephone: (813) 559-4908
Facsimile: (813) 223-5402
jeanmartin@ForThe People.com
rmcgee@ForThe People.com

Attorneys for Plaintiffs

UNITED STATES DISTRICT COURT

CENTRAL DISTRICT OF CALIFORNIA

ALMA FIDELA CERCAS, an individual and California resident, KAITLYN NAKAGOSHI, an individual and Florida resident, JUDY ANNE GRAUSE, an individual and Virginia resident, on behalf of themselves and all others similarly situated,

Plaintiffs,

vs.

AMBRY GENETICS CORP., a Delaware Corporation,

Defendant.

Case No.: _____

CLASS ACTION COMPLAINT

DEMAND FOR JURY TRIAL

Plaintiffs Alma Fidela Cercas ("Cercas"), Kaitlyn Nakagoshi ("Nakagoshi"), and Judy Anne Grause ("Grause") (collectively, "Plaintiffs") bring this Class Action Complaint against

Ambry Genetics Corporation in their respective individual capacities and on behalf of all others similarly situated, and allege, upon personal knowledge as to their own actions and their counsels' investigations, and upon information and belief as to all other matters, as follows:

I. INTRODUCTION

1. Ambry Genetics Corporation ("Ambry" or "Defendant") is a provider of healthcare services throughout the United States. Through its online services, Ambry offers a comprehensive genetic testing menu of more than 300 tests for screening and diagnosis for inherited and non-inherited diseases, such as cancer, heart disease, neurodevelopmental disorders, and other medical issues.

2. On or about April 15, 2020, Ambry announced a security incident involving sensitive personally identifiable information ("PII") and protected health information ("PHI") of its patients (collectively, "Sensitive Information").[1] The exposed Sensitive Information included patients' names, dates of birth, health insurance information, medical information, and for some patients, Social Security Numbers, and other sensitive PII and PHI (the "Data Breach").

3. Although the Data Breach occurred between January 22, 2020 and January 24, 2020, and Ambry reported the Data Breach to government authorities in March 2020, Ambry waited three months before notifying patients.

4. The Data Breach was a direct result of Defendant's failure to implement adequate and reasonable cybersecurity procedures and protocols necessary to protect patients' Sensitive Information.

---

[1] Under the Health Insurance Portability and Accountability Act, 42 U.S.C. § 1320d *et seq.* ("HIPAA"), protected health information ("PHI") is considered to be individually identifiable information relating to the past, present, or future health status of an individual that is created, collected, or transmitted, or maintained by a HIPAA-covered entity in relation to the provision of healthcare, payment for healthcare services, or use in healthcare operations. 45 C.F.R. § 160.103. Health information such as diagnoses, treatment information, medical test results, and prescription information are considered protected health information under HIPAA, as are national identification numbers and demographic information such as birth dates, gender, ethnicity, and contact and emergency contact information. *Summary of the HIPAA Privacy Rule*, *available at*: https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html (last accessed Apr. 21, 2020).

5. Defendant disregarded the rights of Plaintiff and Class Members (defined below) by, among other things, intentionally, willfully, recklessly, or negligently failing to take adequate and reasonable measures to ensure its data systems were protected against unauthorized intrusions; failing to disclose that it did not have reasonable or adequately robust computer systems and security practices to safeguard patients' Sensitive Information; failing to take standard and reasonably available steps to prevent the Data Breach; failing to monitor and timely detect the Data Breach; and failing to provide Plaintiffs and Class Members prompt and accurate notice of the Data Breach.

6. As a result of Defendant's failure to implement and follow reasonable security procedures, patients' Sensitive Information is now in the hands of thieves. Plaintiffs and Class Members have had to spend, and will continue to spend, significant amounts of time and money in an effort to protect themselves from the adverse ramifications of the Data Breach and will forever be at a heightened risk of identity theft and fraud.

7. Plaintiffs, on behalf of all others similarly situated, allege claims for negligence; negligence *per se*; invasion of privacy; breach of implied contract; unjust enrichment; breach of fiduciary duty; breach of confidence; violation of the California Unfair Competition Law (Cal. Business & Professions Code § 17200, *et seq*.); and violation of the Confidentiality of Medical Information Act (Cal. Civ. Code § 56, *et seq*.). Plaintiffs and the Class Members seek to compel Defendant to adopt reasonably sufficient security practices to safeguard patients' Sensitive Information that remains in Defendants' custody to prevent incidents like the Data Breach from reoccurring in the future.

II. PARTIES

8. Plaintiff Alma Fidela Cercas is a resident of Orange County, California, and an Ambry patient. On or about April 15, 2020, Plaintiff Cercas received notice from Ambry that her Sensitive Information had been improperly exposed to unauthorized third parties.

9. Plaintiff Kaitlyn Nakagoshi is a resident of Pinellas County, Florida, and became a patient of Ambry in 2016. In April 2020, Plaintiff Nakagoshi received notice from Ambry that her Sensitive Information had been improperly exposed to unauthorized third parties.

10. Plaintiff Judy Anne Grause is a resident of Roanoke County, Virginia, and an Ambry patient. On or about April 21, 2020, Plaintiff Grause received notice from Ambry that her Sensitive Information had been improperly exposed to unauthorized third parties.

11. Defendant Ambry Genetics Corporation is a Delaware corporation headquartered in Aliso Viejo, CA. Ambry provides genetic testing services, including screening and diagnosis of hereditary cancers and other medical conditions, to patients in the United States. Ambry's parent corporation is Konica Minolta Precision Medicine, Inc.

III. JURISDICTION AND VENUE

12. This Court has subject matter jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). The amount in controversy exceeds $5 million, exclusive of interest and costs, there are more than 100 members in the proposed class, and at least one member of the class is a citizen of a state different from Defendant.

13. Plaintiff Cercas received services from Ambry and engaged in underlying health services within this District where her Sensitive Information was also maintained, and where the Data Breach occurred which led to her sustaining damage. Similarly, Plaintiffs Nakagoshi's and Grause's Sensitive Information was also maintained by Defendant in this District where also the Data Breach occurred which led to them sustaining damage. Through its business operations in this District, Ambry intentionally avails itself of the markets within this District to render the exercise of jurisdiction by this Court just and proper.

14. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(a)(1) because a substantial part of the events and omissions giving rise to this action occurred in this District. Ambry is based in this District, maintains patients' Sensitive Information in the District and has caused harm to Plaintiffs and Class Members residing in this District.

IV. STATEMENT OF FACTS

A. Background.

15. Ambry was founded in 1999 as a basic diagnostic laboratory and has grown over the years to a massive state-of-the-art testing behemoth. The company has performed more than 1 million genetic tests, and is an in-network provider for almost 97% of patients in the U.S. who have public or private health insurance. Ambry's "highly-automated" lab operates 24/7 and performs "DNA fingerprinting of each specimen before and after testing." The comprehensive genetic testing menu of more than 300 tests for screening and diagnosis offered by Ambry includes services for oncology, cardiology, neurology, and exome and general genetics.

16. Patients and healthcare professionals can order tests directly though Ambry's online portal and have the results sent to the doctor or directly to the patient. Patients are billed through their healthcare insurance or personally.[2] Due to the nature of these services, Ambry must keep patients' Sensitive Information in its system. Ambry accomplishes this by keeping the Sensitive Information electronically—even in its email systems, as evidenced by this Data Breach.

17. Patients demand security to safeguard their Sensitive Information. As a healthcare provider, Ambry is required to ensure that such sensitive, personal information is not disclosed or disseminated to unauthorized third parties without the patients' express, written consent, as further detailed below.

[2] Healthcare professionals send Ambry patients' PII and PHI by email to Preverification@ambrygen.com, or by upload through ambrygen.com or portal.ambrygen.com/secure-upload/. *See Ambry's Preverification of Benefits Form, available at:* https://www.ambrygen.com/assets/pdf/billing/preverification_benefits_request_form.pdf (last accessed Apr. 22, 2020).

B. The Data Breach.

18. Beginning on or about April 15, 2020, Ambry sent over 230,000 patients a *Notice of Data Breach*.[3] Thomas Gnielinski, Ambry's Chief Compliance Officer based in Orange County, California, informed the affected patients that:

> Our security team identified unauthorized access to an employee's email account between January 22-24, 2020 . . .. [W]e are notifying you because your personal information may have been impacted. Specifically, while we are not aware of any misuse of your personal information, the security incident may have resulted in the disclosure of your information, including your name, date of birth, Ambry account number, insurance information, and medical information.
>
> We want to assure you that we have taken steps designed to prevent this type of event from happening again, including through an ongoing effort to enhance our security measures and to provide additional training to employees.

19. Ambry's patients' Sensitive Information is likely for sale on the dark web and, on information and belief, is still for sale to criminals. This means that the Data Breach was successful; unauthorized individuals accessed Ambry's patients' unencrypted, unredacted information, including name, date of birth, billing and insurance information, patient referral information, relevant medical records, and more, including Social Security Numbers.

C. Plaintiffs' Efforts to Secure Their Sensitive Information

20. Upon receiving Notice from Ambry on or about April 15, 2020, Plaintiff Cercas signed up with a credit monitoring agency; requested a new medical insurance number; placed fraud alerts on her accounts with all three credit bureaus; and is in the process of contacting the Social Security Administration, and contacting her various doctors to update them with her new insurance number. Plaintiff Cercas is also contacting her bank to further monitor her account.

---

[3] *Ambry Notice of Data Breach,* archived on the California Attorney General's website, *available at*: https://oag.ca.gov/system/files/Sample%20Notification%20Letter_5.pdf (last accessed Apr. 21, 2020); *see also, Ambry's Substitute Notice, available at:* https://www.ambrygen.com/legal/substitute-notice (last accessed Apr. 21, 2020); U.S. Dept. of Health and Human Services, *Cases Currently Under Investigation, available at:* https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf (last accessed Apr. 22, 2020)(stating that Ambry reported the Data Breach to the Department of Health and Human Services on March 22, 2020 as a "Hacking/IT Incident" affecting 232,772 individuals).

This is time Plaintiff Cercas otherwise would have spent performing other activities, such as her job and/or leisurely activities for the enjoyment of life.

21. Knowing that thieves stole her Sensitive Information, potentially including her DNA and genetic medical information, and knowing that her Sensitive Information may be available for sale on the dark web, has caused Plaintiff Cercas great anxiety. She is now very concerned about her healthcare coverage and identity theft in general. This Data Breach has given Plaintiff Cercas hesitation about using electronic services, and reservations about conducting other online activities requiring her personal information.

22. Plaintiff Cercas suffered actual injury from having her Sensitive Information exposed as a result of the Data Breach including, but not limited to: (a) paying monies to Ambry for its goods and services which she would not have, had Ambry disclosed that it lacked data security practices adequate to safeguard consumers' Sensitive Information from theft; (b) damages to and diminution in the value of her Sensitive Information—a form of intangible property that the Plaintiff Cercas entrusted to Ambry as a condition for healthcare services; (c) loss of her privacy; and (d) imminent and impending injury arising from the increased risk of fraud and identity theft.

23. As a result of the Data Breach, Plaintiff Cercas will continue to be at heightened risk for financial fraud, medical fraud and identity theft, and the attendant damages, for years to come.

24. Upon receiving Notice from Ambry in late April 2020, Plaintiff Nakagoshi is considering signing up with a credit monitoring agency and reviewing her credit card and other online statement to check for fraudulent activity. This is time Plaintiff Nakagoshi otherwise would have spent performing other activities, such as her job and/or leisurely activities for the enjoyment of life.

25. Knowing that thieves stole her Sensitive Information, potentially including her DNA and genetic medical information, and knowing that her Sensitive Information may be available for sale on the dark web, has caused Plaintiff Nakagoshi great anxiety. She is now very concerned about her healthcare coverage and identity theft in general. This Data Breach has given

Plaintiff Nakagoshi hesitation about using electronic services, and reservations about conducting other online activities requiring her personal information.

26. Plaintiff Nakagoshi suffered actual injury from having her Sensitive Information exposed as a result of the Data Breach including, but not limited to: (a) paying monies to Ambry for its goods and services which she would not have, had Ambry disclosed that it lacked data security practices adequate to safeguard consumers' Sensitive Information from theft; (b) damages to and diminution in the value of her Sensitive Information—a form of intangible property that the Plaintiff Nakagoshi entrusted to Ambry as a condition for healthcare services; (c) loss of her privacy; and (d) imminent and impending injury arising from the increased risk of fraud and identity theft.

27. As a result of the Data Breach, Plaintiff Nakagoshi will continue to be at heightened risk for financial fraud, medical fraud and identity theft, and the attendant damages, for years to come.

28. Upon receiving Notice from Ambry on or about April 21, 2020, Ms. Grause reviewed her current credit monitoring account and attempted to sign up with the credit monitoring agency supplied by Defendant. She is in the process of notifying her medical insurance providers, placing fraud alerts with all three credit bureaus and contacting the Social Security Administration and her various healthcare providers to alert them of the Data Breach. Ms. Grause is also contacting her bank to further monitor her checking account. This is time Ms. Grause otherwise would have spent performing other activities, such as her job and/or leisurely activities for the enjoyment of life.

29. Knowing that thieves stole her Sensitive Information, and knowing that her Sensitive Information may be available for sale on the dark web, has caused Ms. Grause great anxiety. This Data Breach has caused her to not want to share any PII or PHI electronically, although she understands how difficult that choice is in this age of technology. She now has intense hesitation about using electronic services, and reservations about conducting other online activities requiring her personal information. Ms. Grause is now also very concerned about her healthcare coverage and identity theft in general.

30. Ms. Grause suffered actual injury from having her Sensitive Information exposed as a result of the Data Breach including, but not limited to: (a) paying monies to Ambry for its goods and services which she would not have, had Ambry disclosed that it lacked data security practices adequate to safeguard consumers' Sensitive Information from theft; (b) damages to and diminution in the value of her Sensitive Information—a form of intangible property that the Plaintiff Grause entrusted to Ambry as a condition for healthcare services; (c) loss of her privacy; (d) imminent and impending injury arising from the increased risk of fraud and identity theft.

D. Ambry's Privacy Policies.

31. Ambry maintains policies that detail their promises and legal obligations to maintain and protect patients' Sensitive Information.

32. Ambry's Privacy Policy[4] provides, in part:

> Ambry Genetics Corporation ("Ambry," "we," or "us") is committed to protecting your privacy. We have established this Privacy Policy to inform you of the specific practices and guidelines that protect the security and confidentiality of your personal information. By using our website, ambrygen.com, or any application or online services available on ambrygen.com (collectively, the "Services"), or by transmitting information to us by email or other electronic means, you agree to the terms of this Privacy Policy.
> …
>
> **Security Measures**
>
> Information that you provide to Ambry through ambrygen.com is encrypted using industry standard Secure Sockets Layer (SSL) technology. Your information is processed and stored on controlled servers with restricted access.

33. Ambry's Notice of Privacy Practices[5] provides, in part:

> **We are required by law to:**
>
> - Maintain the confidentiality of your protected health information in accordance with the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") and applicable state law;
> - Comply with the terms of this Notice, including any amendments; and

[4] *Ambry's Privacy Policy, available at*: https://www.ambrygen.com/legal/privacy-policy (last accessed Apr. 21, 2020).

[5] *Ambry Notice of Privacy Practices, available at*: https://www.ambrygen.com/legal/notice-of-privacy-practices (last accessed Apr. 21, 2020).

- Give you this Notice of our legal duties and privacy practices with respect to your PHI that we maintain.

…

Your Authorization Is Needed for Other Uses and Disclosures

Unless otherwise permitted by applicable law, we will not use or disclose your PHI for purposes not described in this Notice unless you give us written authorization to do so (including via electronic signature). If you give us such written authorization, then, in most cases, you may revoke it in writing at any time as described in the authorization. Your revocation will be effective with respect to all of your PHI that we maintain, unless we have already taken action in reliance on your authorization.

34. Ambry also describes how it may use and disclose medical information for each category of uses or disclosures, none of which provide it a right to expose patients' Sensitive Information in the manner it was exposed to unauthorized third parties in the Data Breach.

E. The Healthcare Sector is Particularly Susceptible to Cyber Attacks.

35. The number of U.S. data breaches surpassed 1,000 in 2016, a record high and a forty percent increase in the number of data breaches from the previous year.[6] In 2017, a new record high of 1,579 breaches were reported representing a 44.7 percent increase.[7] That trend continues.

36. The healthcare sector reported the second largest number of breaches among all measured sectors in 2018, with the highest rate of exposure per breach.[8] Indeed, when compromised, healthcare related data is among the most sensitive and personally consequential. A report focusing on healthcare breaches found that the "average total cost to resolve an identity theft-related incident . . . came to about $20,000," and that the victims were often forced to pay

---

[6] Identity Theft Resource Center, *Data Breaches Increase 40 Percent in 2016, Finds New Report From Identity Theft Resource Center and CyberScout* (Jan. 19, 2017), *available at:* https://www.idtheftcenter.org/surveys-studys (last accessed Apr. 21, 2020).

[7] Identity Theft Resource Center, *2017 Annual Data Breach Year-End Review, available at:* https://www.idtheftcenter.org/2017-data-breaches/ (last accessed Apr. 21, 2020).

[8] Identity Theft Resource Center, *2018 End -of-Year Data Breach Report, available at*: https://www.idtheftcenter.org/2018-data-breaches/ (last accessed Apr. 21, 2020).

out-of-pocket costs for healthcare they did not receive in order to restore coverage.[9] Almost 50 percent of the victims lost their healthcare coverage as a result of the incident, while nearly 30 percent said their insurance premiums went up after the event. Forty percent of the customers were never able to resolve their identity theft at all. Data breaches and identity theft have a crippling effect on individuals and detrimentally impact the economy as a whole.[10]

37. Healthcare related data breaches have continued to rapidly increase. According to the 2019 HIMSS Cybersecurity Survey, 82 percent of participating hospital information security leaders reported having a significant security incident in the last 12 months, with a majority of these known incidents being caused by "bad actors" such as cybercriminals.[11] "Hospitals have emerged as a primary target because they sit on a gold mine of sensitive personally identifiable information for thousands of patients at any given time. From social security and insurance policies, to next of kin and credit cards, no other organization, including credit bureaus, have so much monetizable information stored in their data centers."[12]

38. As a healthcare provider, Ambry knew, or should have known, the importance of safeguarding the patients' Sensitive Information entrusted to it and of the foreseeable consequences if its data security systems were breached. This includes the significant costs that would be imposed on Ambry's patients as a result of a breach. Ambry failed, however, to take adequate cybersecurity measures to prevent the Data Breach from occurring.

F. Ambry Acquires, Collects and Stores Plaintiffs' and Class Members' PII/PHI.

39. Ambry acquires, collects, and stores a massive amount of its patients' protected health-related information and other personally identifiable data.

---

[9] Elinor Mills, *Study: Medical identity theft is costly for victims*, CNET (March 3, 2010), *available at:* https://www.cnet.com/news/study-medical-identity-theft-is-costly-for-victims/ (last accessed Apr. 21, 2020).

[10] *Id.*

[11] *2019 HIMSS Cybersecurity Survey, available at*: https://www.himss.org/2019-himss-cybersecurity-survey (last accessed Apr. 21, 2020).

[12] Inside Digital Health, *How to Safeguard Hospital Data from Email Spoofing Attacks*, April 4, 2019, *available at*: https://www.idigitalhealth.com/news/how-to-safeguard-hospital-data-from-email-spoofing-attacks (last accessed Apr. 21, 2020).

40. As a condition of engaging in health services, Ambry requires that these patients entrust them with highly confidential Sensitive Information.

41. By obtaining, collecting, using, and deriving a benefit from Plaintiffs' and Class Members' Sensitive Information, Ambry assumed legal and equitable duties and knew or should have known that it was responsible for protecting Plaintiffs' and Class Members' Sensitive Information from disclosure.

42. Plaintiffs and the Class Members have taken reasonable steps to maintain the confidentiality of their Sensitive Information. Plaintiffs and the Class Members, as current and former patients, relied on Ambry to keep their Sensitive Information confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information.

G. The Value of PII and the Effects of Unauthorized Disclosure.

43. Ambry was well aware that the Sensitive Information it collects is highly sensitive and of significant value to those who would use it for wrongful purposes.

44. Sensitive Information is a valuable commodity to identity thieves. As the FTC recognizes, PII and PHI identity thieves can commit an array of crimes including identify theft, medical and financial fraud.[13] Indeed, a robust "cyber black market" exists in which criminals openly post stolen PII and PHI on multiple underground Internet websites, commonly referred to as the dark web.

45. While credit card information and associated PII and PHI can sell for as little as $1-$2 on the black market, protected health information can sell for as much as $363 according to the Infosec Institute. This is because one's personal health history (e.g., ailments, diagnosis, surgeries, etc.) cannot be changed.[14] PHI is particularly valuable because criminals can use it to

---

[13] Federal Trade Commission, *Warning Signs of Identity Theft, available at:* https://www.consumer.ftc.gov/articles/0271-warning-signs-identity-theft (last accessed Apr. 21, 2020).

[14] Center for Internet Security, *Data Breaches: In the Healthcare Sector, available at:* https://www.cisecurity.org/blog/data-breaches-in-the-healthcare-sector/ (last accessed Apr. 21, 2020).

target victims with frauds and scams that take advantage of the victim's medical conditions or victim settlements. It can be used to create fake insurance claims, allowing for the purchase and resale of medical equipment, or gain access to prescriptions for illegal use or resale.

46. The ramifications of the Ambry's failure to keep its patients' Sensitive Information secure are long lasting and severe. Once Sensitive Information is stolen, fraudulent use of that information and damage to victims may continue for years.

47. At all relevant times, Ambry knew, or reasonably should have known, of the importance of safeguarding Sensitive Information and of the foreseeable consequences if its data security systems were breached, including, the significant costs that would be imposed on patients as a result of a breach.

H. Ambry's Conduct Violates HIPAA.

48. HIPAA requires covered entities to protect against reasonably anticipated threats to the security of PHI. Covered entities must implement safeguards to ensure the confidentiality, integrity, and availability of PHI. Safeguards must include physical, technical, and administrative components.[15]

49. Title II of HIPAA contains what are known as the Administrative Simplification provisions. 42 U.S.C. §§ 1301, *et seq*. These provisions require, among other things, that the Department of Health and Human Services ("HHS") create rules to streamline the standards for handling PII and PHI like the data Defendant left unguarded. The HHS has subsequently promulgated five rules under authority of the Administrative Simplification provisions of HIPAA.

50. Defendant's Data Breach resulted from a combination of insufficiencies that demonstrate Defendant failed to comply with safeguards mandated by HIPAA regulations. Ambry's security failures include, but are not limited to:

[15] HIPAA Journal, *What is Considered Protected Health Information Under HIPAA?, available at:* https://www.hipaajournal.com/what-is-considered-protected-health-information-under-hipaa/ (last accessed Apr. 21, 2020).

a. Failing to ensure the confidentiality and integrity of electronic protected health information that Defendant creates, receives, maintains, and transmits in violation of 45 C.F.R. §164.306(a)(1);

b. Failing to implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights in violation of 45 C.F.R. §164.312(a)(1);

c. Failing to implement policies and procedures to prevent, detect, contain, and correct security violations in violation of 45 C.F.R. §164.308(a)(1);

d. Failing to identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity in violation of 45 C.F.R. §164.308(a)(6)(ii);

e. Failing to protect against any reasonably-anticipated threats or hazards to the security or integrity of electronic protected health information in violation of 45 C.F.R. §164.306(a)(2);

f. Failing to protect against any reasonably anticipated uses or disclosures of electronically protected health information that are not permitted under the privacy rules regarding individually identifiable health information in violation of 45 C.F.R. §164.306(a)(3);

g. Failing to ensure compliance with HIPAA security standard rules by their workforce in violation of 45 C.F.R. §164.306(a)(94);

h. Impermissibly and improperly using and disclosing protected health information that is and remains accessible to unauthorized persons in violation of 45 C.F.R. §164.502, *et seq.*;

i. Failing to effectively train all members of their workforce (including independent contractors) on the policies and procedures with respect to protected health information as necessary and appropriate for the members of their workforce to

carry out their functions and to maintain security of protected health information in violation of 45 C.F.R. §164.530(b) and 45 C.F.R. §164.308(a)(5); and

j. Failing to design, implement, and enforce policies and procedures establishing physical and administrative safeguards to reasonably safeguard protected health information, in compliance with 45 C.F.R. §164.530(c).

I. Ambry Failed to Comply with FTC Guidelines.

51. The Federal Trade Commission ("FTC") has promulgated numerous guides for businesses that highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.[16]

52. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established cybersecurity guidelines for businesses.[17] The guidelines note that businesses should protect the personal customer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct any security problems.

53. The FTC further recommends that companies not maintain PII and PHI longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.[18]

54. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data, treating the failure to employ reasonable and

---

[16] Federal Trade Commission, *Start With Security*, *available at:* https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf (last accessed Apr. 21, 2020).

[17] Federal Trade Commission, *Protecting Personal Information: A Guide for Business*, available at https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last accessed Apr. 21, 2020).

[18] FTC, *Start With Security*, *supra* note 16.

appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

55. Ambry failed to properly implement basic data security practices. Ambry's failure to employ reasonable and appropriate measures to protect against unauthorized access to patients' Sensitive Information constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

56. Ambry was at all times fully aware of its obligation to protect the Sensitive Information of patients because of its position as a trusted healthcare provider. Ambry was also aware of the significant repercussions that would result from its failure to do so.

J. Ambry Failed to Comply with Healthcare Industry Standards.

57. HHS's Office for Civil Rights ("DHHS") notes:

> While all organizations need to implement policies, procedures, and technical solutions to make it harder for hackers to gain access to their systems and data, this is especially important in the healthcare industry. Hackers are actively targeting healthcare organizations, as they store large quantities of highly sensitive and valuable data.[19]

58. DHHS highlights several basic cybersecurity safeguards that can be implemented to improve cyber resilience that require a relatively small financial investment, yet can have a major impact on an organization's cybersecurity posture including: (a) the proper encryption of PII and PHI; (b) educating and training healthcare employees on how to protect PII and PHI; and (c) correcting the configuration of software and network devices.

59. Private cybersecurity firms have also identified the healthcare sector as being particularly vulnerable to cyber-attacks, both because the of value of the PII and PHI which they

[19] HIPAA Journal, Cybersecurity Best Practices for Healthcare Organizations, https://www.hipaajournal.com/important-cybersecurity-best-practices-for-healthcare-organizations/ (last accessed Apr. 21, 2020).

maintain and because as an industry they have been slow to adapt and respond to cybersecurity threats.[20] They too have promulgated similar best practices for bolstering cybersecurity and protecting against the unauthorized disclosure of PII and PHI.

60. Despite the abundance and availability of information regarding cybersecurity best practices for the healthcare industry, Ambry chose to ignore them. These best practices were known, or should have been known by Ambry, whose failure to heed and properly implement them directly led to the Data Breach and the unlawful exposure of Sensitive Information.

K. Plaintiffs and Class Members Suffered Damages.

61. The ramifications of Defendant's failure to keep patients' Sensitive Information secure are long lasting and severe. Once PII and PHI is stolen, fraudulent use of that information and damage to victims may continue for years. Consumer victims of data breaches are more likely to become victims of identity fraud.[21]

62. The Sensitive Information belonging to Plaintiffs and Class Members is private, sensitive in nature, and was left inadequately protected by Defendant who did not obtain Plaintiffs' or Class Members' consent to disclose such Sensitive Information to any other person as required by applicable law and industry standards.

63. The Data Breach was a direct and proximate result of Ambry's failure to: (a) properly safeguard and protect Plaintiff' and Class Members' Sensitive Information from unauthorized access, use, and disclosure, as required by various state and federal regulations, industry practices, and common law; (b) establish and implement appropriate administrative, technical, and physical safeguards to ensure the security and confidentiality of Plaintiff' and Class

---

[20] *See e.g.,* INFOSEC, *10 Best Practices For Healthcare Security, available at:* https://resources.infosecinstitute.com/category/healthcare-information-security/is-best-practices-for-healthcare/10-best-practices-for-healthcare-security/#gref (last accessed Apr. 21, 2020).

[21] *2014 LexisNexis True Cost of Fraud Study, available at:* https://www.lexisnexis.com/risk/downloads/assets/true-cost-fraud-2014.pdf (last accessed Apr. 21, 2020).

Members' Sensitive Information; and (c) protect against reasonably foreseeable threats to the security or integrity of such information.

64. Defendant had the resources necessary to prevent the Data Breach, but neglected to adequately implement data security measures, despite its obligation to protect patient data.

65. Had Defendant remedied the deficiencies in its data security systems and adopted security measures recommended by experts in the field, it would have prevented the intrusions into its systems and, ultimately, the theft of Sensitive Information.

66. As a direct and proximate result of Defendant's wrongful actions and inactions, Plaintiffs and Class Members have been placed at an imminent, immediate, and continuing increased risk of harm from identity theft and fraud, requiring them to take the time which they otherwise would have dedicated to other life demands such as work and family in an effort to mitigate the actual and potential impact of the Data Breach on their lives.

67. The U.S. Department of Justice's Bureau of Justice Statistics found that "among victims who had personal information used for fraudulent purposes, 29% spent a month or more resolving problems" and that "resolving the problems caused by identity theft [could] take more than a year for some victims."[22]

68. In the breach notification letter, Ambry has made an ambiguous and vague offer of identity monitoring service to patients without providing information as to the terms of service, benefits offered, or length of service. This hollow gesture is wholly inadequate to compensate Plaintiffs and Class Members as it fails to address the fact that victims of data breaches and other unauthorized disclosures commonly face multiple years of ongoing identity theft, medical and financial fraud, and it entirely fails to provide sufficient compensation for the unauthorized release and disclosure of Plaintiffs' and Class Members' Sensitive Information.

[22] U.S. Department of Justice, Office of Justice Programs Bureau of Justice Statistics, *Victims of Identity Theft, 2012*, December 2013, *available at*: https://www.bjs.gov/content/pub/pdf/vit12.pdf (last accessed Apr. 21, 2020).

69. As a result of the Defendant's failures to prevent the Data Breach, Plaintiffs and Class Members have suffered, will suffer, and are at increased risk of suffering:

a. The compromise, publication, theft and/or unauthorized use of their Sensitive Information;

b. Out-of-pocket costs associated with the prevention, detection, recovery and remediation from identity theft or fraud;

c. Lost opportunity costs and lost wages associated with efforts expended and the loss of productivity from addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest and recover from identity theft and fraud;

d. The continued risk to their Sensitive Information, which remains in the possession of Defendant and is subject to further breaches so long as Defendant fails to undertake appropriate measures to protect the Sensitive Information in their possession; and

e. Current and future costs in terms of time, effort and money that will be expended to prevent, detect, contest, remediate and repair the impact of the Data Breach for the remainder of the lives of Plaintiffs and Class Members.

70. In addition to a remedy for the economic harm, Plaintiffs and the Class Members maintain an undeniable interest in ensuring that their Sensitive Information is secure, remains secure, and is not subject to further misappropriation and theft.

L. Ambry's Delay in Identifying & Reporting the Breach Caused Additional Harm.

71. It is axiomatic that:

> The quicker a financial institution, credit card issuer, wireless carrier or other service provider is notified that fraud has occurred on an account, the sooner these organizations can act to limit the damage. Early notification can also help

> limit the liability of a victim in some cases, as well as allow more time for law enforcement to catch the fraudsters in the act.[23]

72. Indeed, once a data breach has occurred:

> [o]ne thing that does matter is hearing about a data breach quickly. That alerts consumers to keep a tight watch on credit card bills, insurance invoices, and suspicious emails. It can prompt them to change passwords and freeze credit reports. And notifying officials can help them catch cybercriminals and warn other businesses of emerging dangers. If consumers don't know about a breach because it wasn't reported, they can't take action to protect themselves (internal citations omitted).[24]

73. Although their Sensitive Information was improperly exposed on or about January 22-24, 2020, affected patients were not notified of the Data Breach until mid-April, depriving them of the ability to promptly mitigate potential adverse consequences resulting from the Data Breach.

74. Ambry did notify HHS on or about March 22, 2020, but waited almost an entire month to notify the California Attorney General, Plaintiffs and the Class.[25]

75. As a result of Ambry's delay in detecting and notifying consumers of the Data Breach, the risk of fraud for Plaintiffs and Class Members has been driven even higher.

V. CLASS ALLEGATIONS

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

---

[23] *Identity Fraud Hits Record High with 15.4 Million U.S. Victims in 2016, Up 16 Percent According to New Javelin Strategy & Research Study*, Business Wire, *available at:* https://www.businesswire.com/news/home/20170201005166/en/Identity-Fraud-Hits-Record-High-15.4-Million (last accessed Apr. 21, 2020).

[24] Consumer Reports, *The Data Breach Next Door Security breaches don't just hit giants like Equifax and Marriott. Breaches at small companies put consumers at risk, too*, January 31, 2019, *available at:* https://www.consumerreports.org/data-theft/the-data-breach-next-door/ (last accessed Apr. 21, 2020).

[25] U.S. Department of Health and Human Services, *Cases Currently Under Investigation, available at:* https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf (last accessed Apr. 22, 2020).

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

All individuals whose Sensitive Information was compromised in the data breach first announced by Ambry on or about April 15, 2020 (the "Nationwide Class").

78. The California Subclass that Plaintiff Cercas seeks to represent is initially defined as follows:

All persons residing in California whose Sensitive Information was compromised in the data breach first announced by Ambry on or about April 15, 2020 (the "California Subclass").

79. Excluded from the Class are the following individuals and/or entities: Defendant and Defendant's parents, subsidiaries, affiliates, officers and directors, current or former employees, and any entity in which Defendant have a controlling interest; all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out; any and all federal, state or local governments, including but not limited to their departments, agencies, divisions, bureaus, boards, sections, groups, counsels and/or subdivisions; and all judges assigned to hear any aspect of this litigation, as well as their immediate family members.

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

81. Numerosity, Fed R. Civ. P. 23(a)(1): The Nationwide Class and California Subclass (the "Classes") are so numerous that joinder of all members is impracticable. Defendant have identified thousands of patients whose Sensitive Information may have been improperly accessed in the Data Breach, and the Classes are apparently identifiable within Defendant's records.

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

a. Whether and when Defendant actually learned of the Data Breach and whether their response was adequate;

b. Whether Defendant owed a duty to the Classes to exercise due care in collecting, storing, safeguarding and/or obtaining their Sensitive Information;

c. Whether Defendant breached that duty;

d. Whether Defendant implemented and maintained reasonable security procedures and practices appropriate to the nature of storing Plaintiffs' and Class Members' Sensitive Information;

e. Whether Defendant acted negligently in connection with the monitoring and/or protecting of Plaintiffs' and Class Members' Sensitive Information;

f. Whether Defendant knew or should have known that they did not employ reasonable measures to keep Plaintiffs' and Class Members' Sensitive Information secure and prevent loss or misuse of that Sensitive Information;

g. Whether Defendant adequately addressed and fixed the vulnerabilities which permitted the Data Breach to occur;

h. Whether Defendant caused Plaintiffs and Class Members damages;

i. Whether Defendant violated the law by failing to promptly notify Class Members that their Sensitive Information had been compromised;

j. Whether Plaintiffs' and the Class Members' Sensitive Information were recorded onto Defendant's internet portal on or before March 3, 2020.

k. Whether Plaintiffs and the other Class Members are entitled to actual damages, credit monitoring, and other monetary relief;

l. Whether Defendant violated the California Unfair Competition Law (Business & Professions Code § 17200, *et seq*.); and

m. Whether Defendant violated the Confidentiality of Medical Information Act (Cal. Civ. Code § 56, *et seq*.),

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

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

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

86. Superiority and Manageability, Fed. R. Civ. P. 23(b)(3): The class litigation is an appropriate method for fair and efficient adjudication of the claims involved. Class action treatment is superior to all other available methods for the fair and efficient adjudication of the controversy alleged herein; it will permit a large number of class members to prosecute their common claims in a single forum simultaneously, efficiently, and without the unnecessary duplication of evidence, effort, and expense that hundreds of individual actions would require. Class action treatment will permit the adjudication of relatively modest claims by certain class members, who could not individually afford to litigate a complex claim against large corporations, like Defendant. Further, even for those class members who could afford to litigate such a claim, it would still be economically impractical and impose a burden on the courts.

87. The nature of this action and the nature of laws available to Plaintiffs and the Class make the use of the class action device a particularly efficient and appropriate procedure to afford relief to Plaintiffs and the Class for the wrongs alleged because Defendant would necessarily gain an unconscionable advantage since Defendant would be able to exploit and overwhelm the limited

resources of each individual Class Member with superior financial and legal resources; the costs of individual suits could unreasonably consume the amounts that would be recovered; proof of a common course of conduct to which Plaintiffs were exposed is representative of that experienced by the Class and will establish the right of each Class Member to recover on the cause of action alleged; and individual actions would create a risk of inconsistent results and would be unnecessary and duplicative of this litigation.

88. Ambry is based in Aliso Viejo, California, and on information and belief, all managerial decisions emanate from there, the representations on Defendant's website originate from there, Defendant's misrepresentations originated from California, and therefore application of California law to the Nationwide Class is appropriate.

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

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

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

92. Further, Defendant has acted or refused to act on grounds generally applicable to the Class and, accordingly, final injunctive or corresponding declaratory relief with regard to the Class Members as a whole is appropriate under Rule 23(b)(2) of the Federal Rules of Civil Procedure.

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

a. Whether Defendant owed a legal duty to Plaintiffs and the Class Members to exercise due care in collecting, storing, using, and safeguarding their Sensitive Information;

b. Whether Defendant breached a legal duty to Plaintiffs and the Class Members to exercise due care in collecting, storing, using, and safeguarding their Sensitive Information;

c. Whether Defendant failed to comply with their own policies and applicable laws, regulations, and industry standards relating to data security;

d. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach; and

e. Whether Class Members are entitled to actual damages, credit monitoring or other injunctive relief, and/or punitive damages as a result of Defendant's wrongful conduct.

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

94. Plaintiffs restate and reallege Paragraphs 1 through 93 as if fully set forth herein.

95. As a condition of receiving services, Plaintiffs and Class Members were obligated to provide Ambry directly, or through their respective healthcare providers, with their Sensitive Information.

96. Plaintiffs and the Class Members entrusted their Sensitive Information to Ambry with the understanding that Ambry would safeguard their information.

97. Defendant had full knowledge of the sensitivity of the Sensitive Information and the types of harm that Plaintiffs and Class Members could and would suffer if the Sensitive Information were wrongfully disclosed.

98. Defendant had a duty to exercise reasonable care in safeguarding, securing and protecting such information from being compromised, lost, stolen, misused, and/or disclosed to unauthorized parties. This duty includes, among other things, designing, maintaining and testing

its security protocols to ensure that Sensitive Information in its possession was adequately secured and protected and that employees tasked with maintaining such information were adequately training on relevant cybersecurity measures.

99. Plaintiffs and the Class Members were the foreseeable and probable victims of any inadequate security practices and procedures. Defendant knew of or should have known of the inherent risks in collecting and storing the Sensitive Information of Plaintiffs and the Class, the critical importance of providing adequate security of that Sensitive Information, the current cyber scams being perpetrated, and that it had inadequate employee training and education and IT security protocols in place to secure the Sensitive Information of Plaintiffs and the Class.

100. Defendant's own conduct created a foreseeable risk of harm to Plaintiffs and Class Members. Defendant's misconduct included, but was not limited to, its failure to take the steps and opportunities to prevent the Data Breach as set forth herein. Defendant's misconduct also included its decision not to comply with HIPAA and industry standards for the safekeeping and encrypted authorized disclosure of the Sensitive Information of Plaintiffs and Class Members.

101. Plaintiffs and the Class Members had no ability to protect their Sensitive Information that was in Ambry's possession.

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

103. Defendant had a duty to put proper procedures in place to prevent the unauthorized dissemination of Plaintiffs and Class Members' Sensitive Information.

104. Defendant has admitted that Plaintiffs' and Class Members' Sensitive Information was wrongfully disclosed to unauthorized third persons as a result of the Data Breach.

105. Defendant, through its actions and/or omissions, unlawfully breached its duty to Plaintiffs and Class Members by failing to exercise reasonable care in protecting and safeguarding the Plaintiffs' and Class Members' Sensitive Information while it was within Ambry's possession or control.

106. Defendant improperly and inadequately safeguarded Plaintiffs' and Class Members' Sensitive Information in deviation of standard industry rules, regulations and practices at the time of the Data Breach.

107. Defendant, through its actions and/or omissions, unlawfully breached its duty to Plaintiffs and Class Members by failing to have appropriate procedures in place to detect and prevent dissemination of its patients' Sensitive Information.

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

109. But for Defendant's wrongful and negligent breach of duties owed to Plaintiffs and Class Members, Plaintiffs' and Class Members' Sensitive Information would not have been compromised.

110. There is a temporal and close causal connection between Defendant's failure to implement security measures to protect the Sensitive Information and the harm suffered, or risk of imminent harm suffered, by Plaintiffs and the Class.

111. As a result of Defendant's negligence, Plaintiffs and the Class Members have suffered and will continue to suffer damages and injury including, but not limited to: out-of-pocket expenses associated with procuring robust identity protection and restoration services; increased risk of future identity theft and fraud and the costs associated therewith; time spent monitoring, addressing and correcting the current and future consequences of the Data Breach; and the necessity to engage legal counsel and incur attorneys' fees, costs and expenses.

COUNT II
Negligence *Per Se*
(On Behalf of Plaintiffs and the Nationwide Class)

112. Plaintiffs restate and reallege Paragraphs 1 through 93 as if fully set forth herein.

113. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Ambry, of failing to use reasonable measures to protect Sensitive Information. The FTC publications and orders described above also form part of the basis of Defendant's duty in this regard.

114. Ambry violated Section 5 of the FTC Act by failing to use reasonable measures to protect patients' Sensitive Information and not complying with applicable industry standards, as described in detail herein. Ambry's conduct was particularly unreasonable given the nature and amount of Sensitive Information it obtained and stored, and the foreseeable consequences of a data breach including, specifically, the damages that would result to Plaintiffs and Class Members.

115. Ambry's violation of Section 5 of the FTC Act constitutes negligence *per se*.

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

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

118. Ambry's violation of HIPAA also independently constitutes negligence *per se*.

119. HIPAA privacy laws were enacted with the objective of protecting the confidentiality of patients' healthcare information and set forth the conditions under which such information can be used, and to whom it can be disclosed. HIPAA privacy laws not only apply to healthcare providers and the organizations they work for, but to any entity that may have access to healthcare information about a patient that—if it were to fall into the wrong hands—could present a risk of harm to the patient´s finances or reputation.

120. Plaintiffs and Class Members are within the class of persons that HIPAA privacy laws were intended to protect.

121. The harm that occurred as a result of the Data Breach is the type of harm HIPAA privacy laws were intended to guard against.

122. As a direct and proximate result of Ambry's negligence *per se*, Plaintiffs and the Class have suffered, and continue to suffer, injuries and damages arising from the Data Breach including, but not limited to: damages from lost time and effort to mitigate the actual and potential impact of the Data Breach on their lives, including, *inter alia*, by placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, closing or modifying

financial and medical accounts, closely reviewing and monitoring their credit reports and various accounts for unauthorized activity, filing police reports, and damages from identity theft, which may take months if not years to discover and detect.

123. Additionally, as a direct and proximate result of Ambry's negligence *per se*, Plaintiffs and Class Members have suffered and will suffer the continued risks of exposure of their Sensitive Information, which remains in Ambry's possession and is subject to further unauthorized disclosures so long as Ambry fail to undertake appropriate and adequate measures to protect the Sensitive Information in its continued possession.

COUNT III
Invasion of Privacy
(On Behalf of Plaintiffs and the Nationwide Class)

124. Plaintiffs restate and realleges paragraph 1 through 93 as if fully set forth herein.

125. Plaintiffs and Class Members had a legitimate expectation of privacy with respect to their Sensitive Information and were accordingly entitled to the protection of this information against disclosure to unauthorized third parties.

126. Defendant owed a duty to patients in its network, including Plaintiffs and Class Members, to keep their Sensitive Information confidential.

127. The unauthorized release of Sensitive Information, especially the type related to personal health information, is highly offensive to a reasonable person.

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

129. The Data Breach constitutes an intentional interference with Plaintiffs and Class Members' interest in solitude or seclusion, either as to their persons or as to their private affairs or concerns, of a kind that would be highly offensive to a reasonable person.

130. Defendant acted with a knowing state of mind when it permitted the Data Breach because it knew its information security practices were inadequate.

131. Acting with knowledge, Ambry had notice and knew that its inadequate cybersecurity practices would cause injury to Plaintiffs and Class Members.

132. As a proximate result of Defendant's acts and omissions, Plaintiffs' and Class Members' Sensitive Information was disclosed to and used by third parties without authorization, causing Plaintiffs and Class Members to suffer damages.

133. Unless and until enjoined, and restrained by order of this Court, Defendant's wrongful conduct will continue to cause great and irreparable injury to Plaintiffs and Class Members in that the Sensitive Information maintained by Defendant can be viewed, distributed, and used by unauthorized persons.

134. Plaintiffs and Class Members have no adequate remedy at law for the injuries in that a judgment for monetary damages will not end the invasion of privacy for Plaintiffs and the Class.

COUNT IV
Breach of Implied Contract
(On Behalf of Plaintiffs and the Nationwide Class)

135. Plaintiffs restate and reallege paragraphs 1 through 93 as if fully set forth herein.

136. Plaintiffs and Class Members were required to provide their Sensitive Information, including their names, Social Security numbers, addresses, medical record numbers, dates of birth, telephone numbers, email addresses, and various health related information to Defendant as a condition of their use of Defendant's services.

137. Plaintiffs and Class Members paid money, or money was paid on their behalf, to Defendant in exchange for services, along with Defendant's promise to protect their health information and other Sensitive Information from unauthorized disclosure.

138. In their written privacy policies, Ambry expressly promised Plaintiffs and Class Members that it would only disclose protected health information and other Sensitive Information under certain circumstances, none of which relate to the Data Breach.

139. Ambry promised to comply with HIPAA standards and to make sure that Plaintiffs' and Class Members' health information and other Sensitive Information would remain protected.

140. Implicit in the agreement between Plaintiffs and Class Members and the Defendant to provide protected health information and other Sensitive Information, was Defendant's obligation to: (a) use such Sensitive Information for business purposes only; (b) take reasonable steps to safeguard that Sensitive Information; (c) prevent unauthorized disclosures of the Sensitive Information; (d) provide Plaintiffs and Class Members with prompt and sufficient notice of any and all unauthorized access and/or theft of their Sensitive Information; (e) reasonably safeguard and protect the Sensitive Information of Plaintiffs and Class Members from unauthorized disclosure or uses; and (f) retain the Sensitive Information only under conditions that kept such information secure and confidential.

141. Without such implied contracts, Plaintiffs and Class Members would not have provided their Sensitive Information to Defendant.

142. Plaintiffs and Class Members fully performed their obligations under the implied contract with Defendant, however, Defendant did not.

143. Defendant breached the implied contracts with Plaintiffs and Class Members by failing to:

a. reasonably safeguard and protect Plaintiffs' and Class Members' Sensitive Information, which was compromised as a result of the Data Breach;

b. comply with its promise to abide by HIPAA;

c. ensure the confidentiality and integrity of electronic protected health information that Defendant created, received, maintained, and transmitted in violation of 45 C.F.R 164.306(a)(1);

d. implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights in violation of 45 C.F.R 164.312(a)(1);

e. implement policies and procedures to prevent, detect, contain, and correct security violations in violation of 45 C.F.R 164.308(a)(1);

f. identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity in violation of 45 C.F.R 164.308(a)(6)(ii); and

g. protect against any reasonably anticipated threats or hazards to the security or integrity of electronic protected health information in violation of 45 C.F.R 164.306(a)(2).

144. As a direct and proximate result of Ambry's breach of the implied contracts, Plaintiffs and the Class have suffered, and continue to suffer, injuries and damages arising from the Data Breach including, but not limited to: damages from lost time and effort to mitigate the actual and potential impact of the Data Breach on their lives, including, *inter alia*, by placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, closing or modifying financial and medical accounts, closely reviewing and monitoring their credit reports and various accounts for unauthorized activity, filing police reports, and damages from identity theft, which may take months if not years to discover and detect.

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

145. Plaintiffs restate and reallege paragraphs 1 through 93 as if fully set forth herein.

146. Plaintiffs and Class Members conferred a monetary benefit on Defendant. Specifically, they purchased goods and services from Defendant and in so doing provided Defendant with their Sensitive Information. In exchange, Plaintiffs and Class Members should have received from Defendant the goods and services that were the subject of the transaction and have their Sensitive Information protected with adequate data security.

147. Defendant knew that Plaintiffs and Class Members conferred a benefit which Defendant accepted. Defendant profited from these transactions and used the Sensitive Information of Plaintiffs and Class Members for business purposes.

148. The amounts Plaintiffs and Class Members paid for goods and services were used, in part, to pay for use of Defendant's network and the administrative costs of data management and security.

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

150. Defendant failed to secure Plaintiffs' and Class Members' Sensitive Information and, therefore, did not provide full compensation for the benefit Plaintiffs and Class Members provided.

151. Defendant acquired the Sensitive Information through inequitable means in that it failed to disclose the inadequate security practices previously alleged.

152. If Plaintiffs and Class Members knew that Defendant had not reasonably secured their Sensitive Information, they would not have agreed to Defendant's services.

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

154. As a direct and proximate result of Defendant's conduct, Plaintiffs and Class Members have suffered and will suffer injury, including but not limited to: (a) actual identity theft; (b) the loss of the opportunity of how their Sensitive Information is used; (c) the compromise, publication, and/or theft of their Sensitive Information; (d) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, and/or unauthorized use of their Sensitive Information; (e) lost opportunity costs associated with efforts expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (f) the continued risk to their Sensitive Information, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect Sensitive Information in their continued possession; and (g) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the Sensitive Information

compromised as a result of the Data Breach for the remainder of the lives of Plaintiffs and Class Members.

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

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

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

157. Plaintiffs restate and reallege paragraphs 1 through 93 as if fully set forth herein.

158. In light of their special relationship, Defendant has become the guardian of Plaintiffs' and Class Member's Sensitive Information. Defendant has become a fiduciary, created by its undertaking and guardianship of patients' Sensitive Information, to act primarily for the benefit of its patients, including Plaintiffs and Class Members. This duty included the obligation to safeguard Plaintiffs' and Class Members' Sensitive Information and to timely notify them in the event of a data breach.

159. Defendant has a fiduciary duty to act for the benefit of Plaintiffs and Class Members upon matters within the scope of its relationship. Defendant breached its fiduciary duties owed to Plaintiffs and Class Members by failing to:

a. properly encrypt and otherwise protect the integrity of the system containing Plaintiffs' and Class Members' protected health information and other Sensitive Information;

b. timely notify and/or warn Plaintiffs and Class Members of the Data Breach;

c. ensure the confidentiality and integrity of electronic protected health information Defendant created, received, maintained, and transmitted, in violation of 45 C.F.R 164.306(a)(1);

d. implement technical policies and procedures to limit access to only those persons or software programs that have been granted access rights in violation of 45 C.F.R 164.312(a)(1);

e. implement policies and procedures to prevent, detect, contain, and correct security violations, in violation of 45 C.F.R 164.308(a)(1);

f. identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity in violation of 45 C.F.R 164.308(a)(6)(ii);

g. protect against any reasonably-anticipated threats or hazards to the security or integrity of electronic protected health information in violation of 45 C.F.R 164.306(a)(2);

h. protect against any reasonably anticipated uses or disclosures of electronic protected health information that are not permitted under the privacy rules regarding individually identifiable health information in violation of 45 C.F.R 164.306(a)(3);

i. ensure compliance with the HIPAA security standard rules by its workforce in violation of 45 C.F.R 164.306(a)(94);

j. prevent the improper use and disclosure of protected health information that is and remains accessible to unauthorized persons in violation of 45 C.F.R 164.502, *et seq*.;

k. effectively train all members of its workforce (including independent contractors) on the policies and procedures with respect to protected health information as necessary and appropriate for the members of their workforce to carry out their functions and to maintain security of protected health information in violation of 45 C.F.R 164.530(b) and 45 C.F.R 164.308(a)(5);

l. design, implement, and enforce policies and procedures establishing physical and administrative safeguards to reasonably safeguard protected health information, in compliance with 45 C.F.R 164.530(c); and

m. otherwise failing to safeguard Plaintiffs' and Class Members' Sensitive Information.

160. As a direct and proximate result of Defendant's breaches of its fiduciary duties, Plaintiffs and Class Members have suffered and will suffer injury, including but not limited to: (a) actual identity theft; (b) the loss of the opportunity of how their Sensitive Information is used; (c) the compromise, publication, and/or theft of their Sensitive Information; (d) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft and/or unauthorized use of their Sensitive Information; (e) lost opportunity costs associated with the effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (f) the continued risk to their Sensitive Information, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect patients' Sensitive Information in their continued possession; and (g) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the Sensitive Information compromised as a result of the Data Breach for the remainder of the lives of Plaintiffs and Class Members.

161. As a direct and proximate result of Defendant's breach of its fiduciary duty, Plaintiffs and Class Members have suffered and will continue to suffer other forms of injury and/or harm, and other economic and non-economic losses.

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

162. Plaintiffs restate and reallege paragraphs 1 through 93 as if fully set forth herein.

163. At all times during Plaintiffs' and Class Members' interactions with Defendant, Defendant was fully aware of the confidential and sensitive nature of Plaintiffs' and Class Members' Sensitive Information that Plaintiffs and Class Members provided to Defendant.

164. As alleged herein and above, Defendant's relationship with Plaintiffs and Class Members was governed by terms and expectations that Plaintiffs' and Class Members' Sensitive

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

165. Plaintiffs and Class Members provided their respective Sensitive Information to Defendant with the explicit and implicit understandings that Defendant would protect and not permit the Sensitive Information to be disseminated to any unauthorized parties.

166. Plaintiffs and Class Members also provided their Sensitive Information to Defendant with the explicit and implicit understandings that Defendant would take precautions to protect that Sensitive Information from unauthorized disclosure, such as following basic principles of protecting its networks and data systems, including employees' email accounts.

167. Defendant voluntarily received in confidence Plaintiffs' and Class Members' Sensitive Information with the understanding that the Sensitive Information would not be disclosed or disseminated to the public or any unauthorized third parties.

168. Due to Defendant's failure to prevent, detect, and avoid the Data Breach from occurring by, *inter alia*, following best information security practices to secure Plaintiffs' and Class Members' Sensitive Information, Plaintiffs' and Class Members' Sensitive Information was disclosed and misappropriated to unauthorized third parties beyond Plaintiffs' and Class Members' confidence, and without their express permission.

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

170. But for Defendant's disclosure of Plaintiffs' and Class Members' Sensitive Information in violation of the parties' understanding of confidence, their Sensitive Information would not have been compromised, stolen, viewed, accessed, and used by unauthorized third parties. Defendant's Data Breach was the direct and legal cause of the theft of Plaintiffs' and Class Members' Sensitive Information, as well as the resulting damages.

171. The injury and harm Plaintiffs and Class Members suffered was the reasonably foreseeable result of Defendant's unauthorized disclosure of Plaintiffs' and Class Members' Sensitive Information. Defendant knew its computer systems and technologies for accepting and

securing Plaintiffs' and Class Members' Sensitive Information had numerous security and other vulnerabilities that placed Plaintiffs' and Class Members' Sensitive Information in jeopardy.

172. As a direct and proximate result of Defendant's breaches of confidence, Plaintiffs and Class Members have suffered and will suffer injury, including but not limited to: (a) actual identity theft; (b) the compromise, publication, and/or theft of their Sensitive Information; (c) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft and/or unauthorized use of their Sensitive Information; (d) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (e) the continued risk to their Sensitive Information, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Sensitive Information in its continued possession; (f) future costs in terms of time, effort, and money that will be expended as result of the Data Breach for the remainder of the lives of Plaintiffs and Class Members; and (g) the diminished value of Defendant's services they received.

173. As a direct and proximate result of Defendant's breaches of its fiduciary duties, Plaintiffs and Class Members have suffered and will continue to suffer other forms of injury and/or harm, and other economic and non-economic losses.

COUNT VIII
Violation of the California Unfair Competition Law,
Cal. Bus. & Prof. Code § 17200, *et seq*. – Unlawful Business Practices
(On Behalf of Plaintiffs and the Nationwide Class)

174. Plaintiffs restate and reallege paragraphs 1 through 93 as if fully set forth herein.

175. Defendant has violated Cal. Bus. and Prof. Code § 17200, *et seq*., by engaging in unlawful, unfair or fraudulent business acts and practices and unfair, deceptive, untrue or misleading advertising that constitute acts of "unfair competition" as defined in Cal. Bus. Prof. Code § 17200 with respect to the services provided to the Nationwide Class.

176. Defendant engaged in unlawful acts and practices with respect to the services by establishing the sub-standard security practices and procedures described herein; by soliciting and

collecting Plaintiffs' and Class Members' Sensitive Information with knowledge that the information would not be adequately protected; and by storing Plaintiffs' and Class Members' Sensitive Information in an unsecure electronic environment in violation of HIPAA and California's data breach statute, Cal. Civ. Code § 1798.81.5, which require Defendant to take reasonable methods of safeguarding the Sensitive Information of Plaintiffs and the Class Members.

177. In addition, Defendant engaged in unlawful acts and practices by failing to disclose the Data Breach in a timely and accurate manner, contrary to the duties imposed by Cal. Civ. Code § 1798.82 and Cal. Health & Safety Code §1280.15(b)(2).[26]

178. As a direct and proximate result of Defendant's unlawful practices and acts, Plaintiffs and the Class Members were injured and lost money or property, including but not limited to the price received by Defendant for the services, the loss of Plaintiffs' and Class Members' legally protected interest in the confidentiality and privacy of their Sensitive Information, nominal damages, and additional losses as described herein.

179. Defendant knew or should have known that Defendant's computer systems and data security practices were inadequate to safeguard Plaintiffs' and Class Members' Sensitive Information and that the risk of a data breach or theft was highly likely. Defendant's actions in engaging in the above-named unlawful practices and acts were negligent, knowing and willful, and/or wanton and reckless with respect to the rights of Plaintiffs and the Class Members.

180. Plaintiffs, on behalf of the Class, seek relief under Cal. Bus. & Prof. Code § 17200, *et seq.*, including, but not limited to, restitution to Plaintiffs and Class Members of money or property that Defendant may have acquired by means of Defendant's unlawful, and unfair business practices, restitutionary disgorgement of all profits accruing to Defendant because

---

[26] Ambry's Notice of Privacy acknowledges its duty to report a breach of medical information to affected patients within five (5) business days. https://www.ambrygen.com/assets/pdf/licenses/notice_of_privacy.pdf (last accessed Apr. 22, 2020).

of Defendant's unlawful and unfair business practices, declaratory relief, attorneys' fees and costs (pursuant to Cal. Code Civ. Proc. § 1021.5), and injunctive or other equitable relief.

COUNT IX
Violation of California's Unfair Competition Law,
Cal. Bus. & Prof. Code § 17200, *et seq*. – Unfair Business Practices
(On Behalf of Plaintiffs and the Nationwide Class)

181. Plaintiffs restate and reallege paragraphs 1 through 93 as if fully set forth herein.

182. Defendant engaged in unfair acts and practices with respect to the services by establishing the sub-standard security practices and procedures described herein; by soliciting and collecting Plaintiffs' and Class Members' Sensitive Information with knowledge that the information would not be adequately protected; and by storing Plaintiffs' and Class Members' Sensitive Information in an unsecure electronic environment. These unfair acts and practices were immoral, unethical, oppressive, unscrupulous, unconscionable, and/or substantially injurious to Plaintiffs and Class Members. They were likely to deceive the public into believing their Sensitive Information were securely stored when it was not. The harm these practices caused to Plaintiffs and Class Members outweighed their utility, if any.

183. Defendant engaged in unfair acts and practices with respect to the provision of services by failing to take proper action following the Data Breach to enact adequate privacy and security measures and protect Plaintiffs' and Class Members' Sensitive Information from further unauthorized disclosure, release, data breaches, and theft. These unfair acts and practices were immoral, unethical, oppressive, unscrupulous, unconscionable, and/or substantially injurious to Plaintiffs and Class Members. They were likely to deceive the public into believing their Sensitive Information was securely stored, when it was not. The harm these practices caused to Plaintiffs and the Class Members outweighed their utility, if any.

184. As a direct and proximate result of Defendant's acts of unfair practices, Plaintiffs and Class Members were injured and lost money or property, including but not limited to the price received by Defendant for the services, the loss of Plaintiffs' and Class Members' legally protected interest in the confidentiality and privacy of their Sensitive Information, nominal damages, and additional losses as described above.

185. Defendant knew or should have known that Defendant's computer systems and data security practices were inadequate to safeguard Plaintiffs' and Class Members' Sensitive Information and that the risk of a data breach or theft was highly likely. Defendant's actions in engaging in the above-named unlawful practices and acts were negligent, knowing and willful, and/or wanton and reckless with respect to the rights of Plaintiffs and Class Members.

186. Plaintiffs, on behalf of the Class, seek relief under Cal. Bus. & Prof. Code § 17200, *et seq*., including, but not limited to, restitution to Plaintiffs and Class Members of money or property that the Defendant may have acquired by means of Defendant's unfair business practices, restitutionary disgorgement of all profits accruing to Defendant because of Defendant's unfair business practices, declaratory relief, attorneys' fees and costs (pursuant to Cal. Code Civ. Proc. § 1021.5), and injunctive or other equitable relief.

COUNT X
Violation of the California Confidentiality of Medical Information Act, Cal. Civ. Code § 56, *et seq*.
(On Behalf of Plaintiffs and the Nationwide Class, or alternatively, Plaintiff Cercas and the California Subclass)

187. Plaintiffs restate and reallege paragraphs 1 through 93 as if fully set forth herein.

188. Defendant is a provider of healthcare within the meaning of Civil Code § 56.06(a) and maintains medical information as defined by Civil Code § 56.05.

189. Plaintiffs and the Classes are patients of Defendant, as defined in Civil Code § 56.05(k).

190. Defendant maintains personal medical information of Plaintiffs and the Classes.

191. Defendant has misused and/or disclosed medical information regarding Plaintiffs and the members of the Classes without written authorization compliant with the provisions of Civil Code §§ 56, *et seq*.

192. Defendant's misuse and/or disclosure of medical information regarding the Plaintiffs and the Classes constitutes a violation of Civil Code §§ 56.10, 56.11, 56.13, and 56.26.

193. Plaintiffs and the Classes have suffered damages from the improper misuse as detailed herein.

PRAYER FOR RELIEF

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

A. An order certifying the Nationwide Class and California Subclass as defined herein, and appointing Plaintiffs and their Counsel to represent the Class;

B. An order enjoining Defendant from engaging in the wrongful conduct alleged herein concerning disclosure and inadequate protection of Plaintiffs' and Class Members' Sensitive Information;

C. An award of compensatory, statutory, and punitive damages, in an amount to be determined;

D. An award for equitable relief requiring restitution and disgorgement of the revenues wrongfully retained as a result of Defendant's wrongful conduct;

E. An award of reasonable attorneys' fees, costs, and litigation expenses, as allowable by law; and

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

Date: April 23, 2020

Respectfully Submitted,

By: /s/ Daniel S. Robinson

Daniel S. Robinson (SBN 244245)
Wesley K. Polischuk (SBN 254121)
Michael W. Olson (SBN 312857)
ROBINSON CALCAGNIE, INC.
19 Corporate Plaza Drive
Newport Beach, CA 92660
(949) 720-1288; Fax (949) 720-1292
drobinson@robinsonfirm.com
wpolischuk@robinsonfirm.com
molson@robinsonfirm.com

Jean S. Martin (Pro Hac Vice Forthcoming)
jeanmartin@ForThePeople.com
Ryan J. McGee (Pro Hac Vice Forthcoming)
rmcgee@ForThePeople.com
MORGAN & MORGAN
COMPLEX LITIGATION GROUP
201 N. Franklin Street, 7th Floor

Tampa, Florida 33602
Telephone: 813-559-4908
Facsimile: (813) 222-4795

M. Anderson Berry (SBN 262879)
aberry@justice4you.com
Leslie Guillon (SBN 222400)
lguillon@justice4you.com
CLAYEO C. ARNOLD,
A PROFESSIONAL LAW CORPORATION
865 Howe Avenue
Sacramento, CA 95825
Telephone: (916) 777-7777
Facsimile: (916) 924-1829

Attorneys for Plaintiffs and the Proposed Classes

DEMAND FOR JURY TRIAL

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

Date: April 23, 2020

Respectfully Submitted,

By: /s/ Daniel S. Robinson

Daniel S. Robinson (SBN 244245)
Wesley K. Polischuk (SBN 254121)
Michael W. Olson (SBN 312857)
ROBINSON CALCAGNIE, INC.
19 Corporate Plaza Drive
Newport Beach, CA 92660
(949) 720-1288; Fax (949) 720-1292
drobinson@robinsonfirm.com
wpolischuk@robinsonfirm.com
molson@robinsonfirm.com

Jean S. Martin (Pro Hac Vice Forthcoming)
jeanmartin@ForThePeople.com
Ryan J. McGee (Pro Hac Vice Forthcoming)
rmcgee@ForThePeople.com
MORGAN & MORGAN
COMPLEX LITIGATION GROUP
201 N. Franklin Street, 7th Floor
Tampa, Florida 33602
Telephone: 813-559-4908
Facsimile: (813) 222-4795

M. Anderson Berry (SBN 262879)
aberry@justice4you.com
Leslie Guillon (SBN 222400)
lguillon@justice4you.com
CLAYEO C. ARNOLD,
A PROFESSIONAL LAW CORPORATION
865 Howe Avenue
Sacramento, CA 95825
Telephone: (916) 777-7777
Facsimile: (916) 924-1829

Attorneys for Plaintiffs and the Proposed Classes