Brian D. Chase (SBN 164109)
bchase@bisnarchase.com
Jerusalem F. Beligan (SBN 211258)
jbeligan@bisnarchase.com
Ian M. Silvers (SBN 247416)
isilvers@bisnarchase.com
BISNAR | CHASE LLP
1301 Dove Street, Suite 120
Newport Beach, California 92660
Telephone: (949) 752-2999
Facsimile: (949) 752-2777

Robert L. Esensten (SBN 65728)
resensten@esenstenlaw.com
Jordan S. Esensten (SBN 264645)
jesensten@esenstenlaw.com
ESENSTEN LAW
12100 Wilshire Boulevard, Suite 1660
Los Angeles, California 90025
Telephone: (310) 279-3090
Facsimile: (310) 207-5969

Counsel for Plaintiff and Putative Class

UNITED STATES DISTRICT COURT

CENTRAL DISTRICT OF CALIFORNIA

JOHANNA A. MAYER, individually, and on behalf of all others similarly situated,

Plaintiff,

vs.

QUEST DIAGNOSTICS, INC.; OPTUM360 SERVICES, INC.; AMERICAN MEDICAL COLLECTION AGENCY and DOES 1 through 100,

Defendants.

Case No.

CLASS ACTION COMPLAINT AND DEMAND FOR JURY TRIAL

Plaintiff Johanna A. Mayer ("Plaintiff"), individually, and on behalf of the class defined below, brings this class action complaint against Quest Diagnostics Inc. ("Quest Diagnostics"), American Medical Collection Agency ("AMCA"), Optum360 LLC ("Optum360"), and Does 1 through 100 ("Doe Defendants") (collectively, Quest Diagnostics, AMCA, Optum 360, and Doe Defendants are referred to as "Defendants") and alleges as follows:

INTRODUCTION

1. On June 3, 2019, Quest Diagnostics, one of the largest blood testing providers in the country, announced a data breach whereby nearly 12 million of its customers, including Plaintiff and putative Class members, had their personally identifiably information ("PII") and protected health information ("PHI") accessed by unauthorized parties due to the negligent data security of AMCA, one if its billing collections vendors (the "Data Breach"). Specifically, the PII and PHI accessed included, but was not limited to, Plaintiff's and Class members' personal information (e.g. Social Security Numbers), financial information (credit card numbers and bank account information), and medical information.

2. In its SEC filing relating to the Data Breach, Quest Diagnostics announced that unauthorized parties accessed between August 1, 2018 and March 30, 2019 AMCA's system, which contained Plaintiff's and Class members' PII and PHI.

3. Despite unauthorized parties having access to the AMCA system for more than six months, AMCA only learned of the Data Breach as a result of receiving information from a security compliance firm that works with credit card companies.

4. Given AMCA's relationship to Question Diagnostics (AMCA provides services to Optum360, which in turn provides payment services to Quest Diagnostics), Plaintiff and Class members were blindsided by the Data Breach announcement given most have never heard of AMCA or Optum360 and were unaware that their information would be shared with these entities, causing additional emotional harm.

5. Based on information and belief, AMCA informed Quest Diagnostics and

Optum360 of the Data Breach on May 14, 2019. Still, Quest Diagnostics and Optum360 waited more than two weeks to notify Plaintiff and Class members of the Data Breach.

6. Based on further information and belief, AMCA first learned of the Data Breach on or around March 30, 2019 but waited more than three months to notify Plaintiff and Class members of the Data Breach.

7. While nearly 12 million Data Breach victims sought out and/or paid for diagnostics testing and medical care from Defendants, thieves were hard at work, stealing and using their hard-to-change Social Security numbers and highly sensitive PII/PHI for nearly one year without the victims' knowledge. Defendants' lax security practices that allowed this intrusion to occur have worsened Plaintiff's and other Class members' lives by, among other injuries: (a) adding to their already heightened financial obligations by placing them at increased risk of fraudulent charges; (b) complicating diagnosis, prognosis, and treatment for their severe medical conditions by placing them at increased risk of having inaccurate medical information in their files; and/or (c) increasing the risk of other potential personal, professional, or financial harms that could be caused as a result of having their PII/PHI exposed.

8. Prior to the Data Breach, Quest Diagnostics acknowledged in its Notice of Privacy Practices that it is "committed to protecting the privacy of your identifiable health information" and that it would only use Plaintiff and Class members PII/PHI for certain limited purposes, such as for treatment, payment, or healthcare operations purposes and for other purposes permitted or required by law. Quest Diagnostics represented that it would abide by these obligations, but failed to live up to its own promises as well as its duties and obligations required by law and industry standards.

9. Contrary to its promises to help patients improve the quality of their lives through secure data practices, Defendants' conduct has instead been a direct cause of the ongoing harm to Plaintiff and other Class members whose suffering has been magnified by the Data Breach, and who will continue to experience harm and data insecurity for the indefinite future.

10. Specifically, Defendants failed to maintain reasonable and/or adequate security measures to protect Plaintiff's and other Class members' PII/PHI from unauthorized access and disclosure, apparently lacking, at a minimum: (1) reasonable and adequate security measures designed to prevent this attack even though Defendants knew or should have known that it was a prized target for hackers; and (2) reasonable and adequate security protocols to promptly detect the unauthorized intrusion into and removal of PII/PHI from its provider database pertaining to nearly 12 million Data Breach victims.

11. Armed with PII/PHI, hackers can sell the PII/PHI to other thieves or misuse themselves to commit a variety of crimes that harm victims of the Data Breach. For instance, they can take out loans, mortgage property, open financial accounts, and open credit cards in a victim's name; use a victim's information to obtain government benefits or file fraudulent returns to obtain a tax refund; obtain a driver's license or identification card in a victim's name; gain employment in another person's name; give false information to police during an arrest; or engage in medical fraud that can result in a harmful misdiagnosis to Plaintiff and Class members.

12. As a result of Defendants' willful failure to prevent the Data Breach, Plaintiff and Class members are more susceptible to identity theft and have experienced, will continue to experience, and face an increased risk of financial harms, in that they are at substantial risk of identity theft, fraud, and other harm.

PARTIES

13. Plaintiff Johanna A. Mayer is a resident and citizen of Lake Elsinore, California. Plaintiff is a customer of Quest Diagnostics, having used Quest Diagnostics at a Lake Elsinore location in Riverside County, California. As a result of Defendants' actions, Plaintiff Mayer has been injured and has financial losses and will be subject to a substantial risk for further identity theft due to Defendants' Data Breach. As a further result of Defendants' actions, Plaintiff Mayer is contemplating purchasing credit monitoring and taking other measures to protect herself from identity theft and fraud.

Plaintiff believed, at the time of using Quest Diagnostics, that it would maintain the privacy and security of her PII/PHI. Plaintiff further believes she paid a premium to Quest Diagnostics for its data security. Plaintiff Mayer would not have used Quest Diagnostics had she known that it would expose, or allow to be exposed, her PII/PHI, making it available to unauthorized parties.

14. Defendant Quest Diagnostics Inc. is a Delaware corporation with its principal place of business in Secaucus, New Jersey.

15. Based on information and belief, Defendant Optum360 Services, Inc. is a Delaware corporation with its principal place of business in Eden Praire, Minnesota.

16. Defendant American Medical Collection Agency is a business with its principal place of business in Elmsford, New York.

17. The true names and/or capacities, whether individual, corporate, partnership, associate or otherwise, of the Defendants herein designated as Does 1 to 100 are unknown to Plaintiff at this time who, therefore, sues said Defendants by fictitious names. Plaintiff alleges that each named Defendant herein designated as Does is negligently, willfully or otherwise legally responsible for the events and happenings herein referred to and proximately caused damages to Plaintiff as herein alleged. Plaintiff will seek leave of Court to amend this Complaint to insert the true names and capacities of such Defendants when they have been ascertained and will further seek leave to join said Defendants in these proceedings.

18. Plaintiff are informed and believe and thereon alleges that at all times mentioned herein, Does were agents, servants, employees, partners, distributors or joint ventures of each other and that in doing the acts herein alleged, were acting within the course and scope of said agency, employment, partnership, or joint venture. Each and every Defendant aforesaid was acting as a principal and was negligent or grossly negligent in the selection, hiring and training of each and every other Defendant or ratified the conduct of every other Defendant as an agent, servant, employee or joint venture.

JURISDICTION AND VENUE

19. This Court has subject matter jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d). This lawsuit is a class action with an amount in controversy over $5 million, involving over 100 proposed class members, some of whom are from a different state than Defendants.

20. This Court may exercise personal jurisdiction over Defendants because they are registered to do business and/or conduct business in California, and the wrongful acts alleged in this complaint were committed in California, among other venues.

21. Venue is proper in this District under 28 U.S.C. § 1391 because a substantial part of the events or omissions giving rise to Plaintiff's claims occurred in this District, and Quest Diagnostics has at least 33 facilities in the State of California, and Defendants are subject to personal jurisdiction in this District.

FACTUAL ALLEGATIONS

A. The Data Breach

22. Beginning around August 1, 2018, unauthorized parties accessed the AMCA system that contained Plaintiff's and Class members' PII and PHI. Plaintiff and Class members are customers who paid and provided their PII and PHI to Quest Diagnostics in exchange for diagnostic and medical services. Quest Diagnostics provided Plaintiff and Class members' PII and PHI to Optum360 who in turn provided that information to AMCA for billing and collection purposes.

23. For more than six months, unauthorized parties maintained uninterrupted access to the AMCA system, containing the PII and PHI of nearly 12 million customers of Quest Diagnostics.

24. According to AMCA, a third-party credit card companies discovered the Data Breach and informed AMCA who confirmed the Data Breach after an internal review. Based on information and belief, AMCA learned about the Data Breach on or around March 30, 2019.

25. AMCA waited until May 14, 2019, to inform Quest Diagnostics and Optum360 of the Data Breach, who then waited more than two weeks to inform Plaintiff and Class members, only doing so through a June 3, 2019 SEC filing.

26. As a result, unauthorized parties have accessed and acquired Plaintiff and Class members' PII and PHI, including, but not limited to, their personal information (e.g. Social Security Numbers), financial information (credit card numbers and bank account information), and medical information.

27. Quest Diagnostics makes numerous promises to its customers that it will maintain the security and privacy of their personal information. For instance, in its Notice of Privacy Practices, Quest Diagnostics promises its customers that it is "committed to protecting the privacy of your identifiable health information."

28. Quest Diagnostics also acknowledges the following:

> Quest Diagnostics is required by law to maintain the privacy of your PHI. We are also required to provide you with this Notice of our legal duties and privacy practices upon request. It describes our legal duties, privacy practices and your patient rights as determined by the Health Insurance Portability and Accountability Act of 1996 (HIPAA). We are required to follow the terms of this Notice currently in effect. We are required to notify affected individuals in the event of a breach involving unsecured protected health information. PHI is stored electronically and is subject to electronic disclosure. This Notice does not apply to non-diagnostic services that we perform such as certain drugs of abuse testing services and clinical trials testing services.

29. Quest Diagnostics also ensures its customers it will only use their PII and PHI for certain limited purposes, such as "for treatment, payment, or healthcare operations purposes and for other purposes permitted or required by law." Quest Diagnostics further provides the following:

> need your written authorization to use or disclose your health information for any purpose not covered by one of the categories below. Subject to compliance with limited exceptions, we will not use or disclose psychotherapy notes, use or disclose your PHI for marketing purposes or sell your PHI, unless you have signed an authorization. You may revoke any authorization you sign at any time. If you revoke

> your authorization, we will no longer use or disclose your health information for the reasons stated in your authorization except to the extent we have already taken action based on your authorization.

30. By failing to protect Plaintiff and Class member's PII and PHI, and by allowing the Data Breach to occur, Quest Diagnostics broke these privacy promises.

31. To date, Defendants have not yet provided a Notice of Data Breach and have not adequately explained how the Data Breach occurred and why it took a third party to inform it of the Data Breach.

B. Personal Identifiable Information/Protected Health Information

32. PII/PHI is of great value to hackers and cyber criminals and the data compromised in the Data Breach can be used in a variety of unlawful manners.

33. PII/PHI is information that can be used to distinguish, identify, or trace an individual's identity, such as their name, Social Security number, and biometric records. This can be accomplished alone, or in combination with other personal or identifying information that is connected, or linked to an individual, such as their birthdate, birthplace, and mother's maiden name.

34. PII/PHI does not include only data that can be used to directly identify or contact an individual (e.g., name, e-mail address), or personal data that is especially sensitive (e.g., Social Security number, bank account number, payment card numbers).

35. PHI—like the type disclosed in the breach—is particularly valuable for cybercriminals. According to SecureWorks (a division of Dell Inc.), "[i]t's a well known truism within much of the healthcare data security community that an individual healthcare record is worth more on the black market ($50, on average) than a U.S.-based credit card and personal identity with social security number combined." The reason is that thieves "[c]an use a healthcare record to submit false medical claims (and thus obtain free medical care), purchase prescription medication, or resell the record on the black market."

36. Similarly, the FBI Cyber Division, in a April 8, 2014 Private Industry Notification, advised:

> Cyber criminals are selling [medical] information on the black market at a rate of $50 for each partial EHR, compared to $1 for a stolen social security number or credit card number. EHR can then be used to file fraudulent insurance claims, obtain prescription medication, and advance identity theft. EHR theft is also more difficult to detect, taking almost twice as long as normal identity theft.

37. Given the nature of the Data Breach, it is foreseeable that the compromised PII/PHI will be used to access Plaintiff and the Class members' financial accounts, thereby providing access to additional PII/PHI or personal and sensitive information. Therefore, the compromised PII/PHI in the Data Breach is of great value to hackers and thieves and can be used in a variety of ways. Information about, or related to, an individual for which there is a possibility of logical association with other information is of great value to hackers and thieves. Indeed, "there is significant evidence demonstrating that technological advances and the ability to combine disparate pieces of data can lead to identification of a consumer, computer or device even if the individual pieces of data do not constitute PII."[1] For example, different PII/PHI elements from various sources may be able to be linked in order to identify an individual, or access additional information about or relating to the individual.

38. Further, as technology advances, computer programs may scan the Internet with wider scope to create a mosaic of information that may be used to link information to an individual in ways that were not previously possible. This is known as the "mosaic effect."[2]

39. Names and dates of birth, combined with contact information like telephone numbers and email addresses, are very valuable to hackers and identity

[1] Fed. Trade Comm'n, Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers, Preliminary FTC Staff Report 35-38 (Dec. 2010) <https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-bureau-consumer-protection-preliminary-ftc-staff-report-protecting-consumer/101201privacyreport.pdf> [as of June 24, 2017].

[2] Fed. Chief Information Officers Council, Recommendations for Standardized Implementation of Digital Privacy Controls (Dec. 2012) pp. 7-8.

thieves as it allows them to access users' other accounts particularly when they have easily-decrypted passwords and security questions.

40. The PII/PHI Defendants exposed is of great value to hackers and cyber criminals and the data compromised in the Data Breach can be used in a variety of unlawful manners, including opening new credit and financial accounts in users' names, obtaining protected health information, and/or committing medical fraud.

41. Unfortunately for Plaintiff and Class members, a person whose PII/PHI has been compromised may not fully experience the effects of the breach for years to come:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[3]

42. Accordingly, Plaintiff and Class members will bear a heightened risk of injury for years to come. Identity theft is one such risk and occurs when an individuals' PII/PHI is used without his or her permission to commit fraud or other crimes.[4]

43. According to the Federal Trade Commission, "the range of privacy-related harms is more expansive than economic or physical harm or unwarranted intrusions and that any privacy framework should recognize additional harms that might arise from unanticipated uses of data."[5]

---

[3] G.A.O., Personal Information: Data Breaches are Frequent, but Evidence of Resulting Identity Theft is Limited; However, the Full Extent is Unknown (June 2007) <http://www.gao.gov/assets/270/262904.html.> [as of June 24, 2017].

[4] Fed. Trade Comm'n, Taking Charge: What To Do If Your Identity Is Stolen (April 2013) <https://www.consumer.ftc.gov/articles/pdf-0014-identity-theft.pdf> [as of June 24, 2017].

[5] Fed. Trade Comm'n, Protecting Consumer Privacy in an Era of Rapid Change (March 2012) <https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf> [as of June 24, 2017].

C. HIPAA Provides Guidelines on How Healthcare Providers Must Secure Patients' Protected Health Information

44. As a healthcare provider, Defendants are subject to the HIPAA Privacy Rule ("Standards for Privacy of Individually Identifiable Health Information"), 45 C.F.R. Part 160 and Part 164, Subparts A and E, and the HIPAA Security Rule ("Security Standards for the Protection of Electronic Protected Health Information"), 45 C.F.R. Part 160 and Part 164, Subparts A and C (collectively, "Privacy and Security Rules").

45. The Privacy and Security Rules establish a national set of standards for the protection of "individually identifiable health information" that is held or transmitted by a health care provider, which HIPAA refers to as "protected health information."

46. Pursuant to HIPAA, Defendants must maintain reasonable and appropriate administrative, technical, and physical safeguards for protecting PHI.

47. HIPAA imposes general security standards that Defendants must follow, including:

a. Ensuring the confidentiality, integrity, and availability of all electronic protected health information the covered entity or business associate creates, receives, maintains, or transmits, 45 C.F.R. § 164.306(a);

b. Protecting against any reasonably anticipated threats or hazards to the security or integrity of such information, 45 C.F.R. § 164.306(a);

c. Protecting against any reasonably anticipated uses or disclosures of such information that are not permitted or required under HIPAA, 45 C.F.R. § 164.306(a); and

d. Reviewing and modifying the security measures implemented under HIPAA as needed to continue provision of reasonable and appropriate protection of electronic protected health information, 45 C.F.R. § 164.306(e).

48. From a technical standpoint, HIPAA requires Defendants to, among other things:

a. Implement technical policies and procedures for electronic information systems that maintain electronic PHI to allow access only to those persons or software programs that have been granted access rights, 45 C.F.R. § 164.312(a);

b. Implement procedures to verify that a person or entity seeking access to electronic PHI is the one claimed, 45 C.F.R. § 164.312(d); and

c. Implement technical security measures to guard against unauthorized access to electronic PHI that is being transmitted over an electronic communications network, 45 C.F.R. § 164.312(e).

49. The HIPAA Security Rule requires Defendants to implement reasonable and appropriate policies and procedures to comply with the standards, implementation specifications, or other requirements of the HIPAA Security Rule. 45 CFR 164.316(a). These policies and procedures must be maintained in written form. 45 CFR 164.316(b)(1)(i).

50. The HIPAA Security Rule requires covered entities to maintain a written record of any action, activity, or assessment required to be documented by the HIPAA Security Rule. 45 CFR 164.316(b)(1)(ii).

51. The HIPAA Security Rule requires covered entities to review documentation periodically and update it as needed, in response to environmental or operational changes affecting the security of the electronic protected health information. 45 CFR 164.316(b)(1)(iii).

52. Under the HIPAA Privacy Rule, Defendants may not use or disclose PHI or confidential medical information except as expressly permitted. 45 CFR 164.502(a).

D. The HITECH Act Provides Additional Guidelines on How Healthcare Providers Must Secure Patients' Protected Health Information

53. The HITECH Act, enacted as part of the American Recovery and Reinvestment Act of 2009 (ARRA) (Pub.L. 111–5), promotes the adoption and meaningful use of health information technology. Subtitle D of the HITECH Act

addresses the privacy and security concerns associated with the electronic transmission of health information.

54. The HITECH Act provides lucrative financial incentives, and the avoidance of penalties, to healthcare entities such as Defendants for demonstrating the meaningful use, interoperability, and security of electronic health information. Achieving meaningful use requires compliance with objectives, measures and certification and standards criteria. The Electronic Health Records ("EHR") Incentive Program requires compliance with the objective to protect electronic health information. A Core Measure to determine compliance with the objective is conducting or reviewing a security risk analysis in accordance with the requirements under 45 CFR 164.308(a)(1) (the HIPAA Security Rule) and implementing security updates as necessary and correcting identified security deficiencies as part of its risk management process.

55. Upon information and belief, Defendants implanted a rushed and substandard EHR infrastructure in order to, in part, obtain millions of dollars in lucrative financial incentives, as well as the avoidance of penalties, despite knowing they were ill-equipped and unprepared to safely store and meaningfully use electronic health records and electronic health information in a secure manner consistent with regulations and industry standards.

E. Defendants are Subject To Other Federal and State Laws and Regulations That Provide Guidelines on the Practices It Should Have Implemented To Secure Patients' Protected Health Information

56. Section 5(a) of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45, prevents Defendants from using "unfair or deceptive acts or practices in or affecting commerce." The FTC has found that inadequate data privacy and cybersecurity practices can constitute unfair or deceptive practices that violate § 5.

57. The state of California generally prohibits healthcare providers from disclosing a patient's confidential medical information without prior authorization. The California Confidentiality of Medical Information Act ("CMIA") (Cal. Civ. Code §

56.10(a)) states that "a provider of health care, health care service plan, or contractor shall not disclose medical information regarding a patient of the provider of health care or enrollee or subscriber of a health care service plan without first obtaining an authorization except as provided in subdivision (b) or (c)." See also Cal. Civ. Code §§ 1798.80, et seq.

58. In addition to their obligations under federal and state laws and regulations, Defendants owed a common law duty to Plaintiff and Class members to protect PII/PHI entrusted to it, including to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the PII/PHI in its possession from being compromised, lost, stolen, accessed, and misused by unauthorized parties.

59. Defendants further owed and breached its duty to Plaintiff and the Class to implement processes and specifications that would detect a breach of its security systems in a timely manner and to timely act upon warnings and alerts, including those generated by its own security systems (e.g. 45 CFR §§ 164.308(a), 164.306(d), 164.312, The Office for Civil Rights July 14, 2010 Guidance on Risk Analysis Requirements under the HIPAA Security Rule, etc.).

60. As a direct and proximate result of Defendants' reckless and negligent actions, inaction, and omissions, the resulting Data Breach, the unauthorized release and disclosure of Plaintiff's and Class members' PII/PHI, and Defendants' failure to properly and timely notify Plaintiff and Class members, Plaintiff and Class members are more susceptible to identity theft and have experienced, will continue to experience and will face an increased risk of experiencing the following injuries, *inter alia*:

a. money and time expended to prevent, detect, contest, and repair identity theft, fraud, and/or other unauthorized uses of personal information;

b. money and time lost as a result of fraudulent access to and use of their financial accounts;

c. loss of use of and access to their financial accounts and/or credit;

d. money and time expended to avail themselves of assets and/or credit

frozen or flagged due to misuse;

e. impairment of their credit scores, ability to borrow, and/or ability to obtain credit;

f. lowered credit scores resulting from credit inquiries following fraudulent activities;

g. money, including fees charged in some states, and time spent placing fraud alerts and security freezes on their credit records;

h. costs and lost time obtaining credit reports in order to monitor their credit records;

i. anticipated future costs from the purchase of credit monitoring and/or identity theft protection services;

j. costs and lost time from dealing with administrative consequences of the Data Breach, including by identifying, disputing, and seeking reimbursement for fraudulent activity, canceling compromised financial accounts and associated payment cards, and investigating options for credit monitoring and identity theft protection services;

k. money and time expended to ameliorate the consequences of the filing of fraudulent tax returns;

l. lost opportunity costs and loss of productivity from efforts to mitigate and address the adverse effects of the Data Breach including, but not limited to, efforts to research how to prevent, detect, contest, and recover from misuse of their personal information;

m. loss of the opportunity to control how their personal information is used; and

n. continuing risks to their personal information, which remains subject to further harmful exposure and theft as long as Defendants fail to undertake appropriate, legally required steps to protect the personal information in its possession.

61. The risks associated with identity theft are serious. "While some identity

theft victims can resolve their problems quickly, others spend hundreds of dollars and many days repairing damage to their good name and credit record. Some consumers victimized by identity theft may lose out on job opportunities, or denied loans for education, housing or cars because of negative information on their credit reports. In rare cases, they may even be arrested for crimes they did not commit."[6]

62. Further, criminals often trade stolen PII/PHI on the "cyber black-market" for years following a breach. Cybercriminals can post stolen PII/PHI on the internet, thereby making such information publicly available.

CLASS ACTION ALLEGATIONS

63. Plaintiff brings all claims as class claims under Federal Rule of Civil Procedure 23(b)(1), (b)(2), (b)(3), and (c)(4).

A. Nationwide Class

64. Plaintiff brings all claims on behalf of a proposed nationwide class ("Nationwide Class"), defined as follows:

> *All persons in the United States whose PII/PHI was compromised as a result of the Data Breach.*

B. California Sub-Class

65. Plaintiff brings all claims on behalf of a proposed California Sub-Class, defined as follows:

> *All persons in the state of California whose PII/PHI was compromised as a result of the Data Breach.*

66. Excluded from the above Classes are Defendants, any entity in which Defendants have a controlling interest or that have a controlling interest in Defendants, and Defendants' legal representatives, assignees, and successors. Also excluded are the Judge to whom this case is assigned and any member of the Judge's immediate family.

[6] True Identity Protection: Identity Theft Overview, ID Watchdog <http://www.idwatchdog.com/tikia//pdfs/Identity-Theft-Overview.pdf> [as of Sept. 23, 2016].

67. **Numerosity:** The Nationwide Class is so numerous that joinder of all members is impracticable. Based on information and belief, the Nationwide Class includes nearly 12 million individuals from across the country who had their PII/PHI compromised, stolen, and published during the Data Breach. The parties will be able to identify the exact size of the class through discovery and Defendants' own documents.

68. **Commonality:** There are numerous questions of law and fact common to Plaintiff and the Nationwide Class including, but not limited to, the following:

- whether Defendants engaged in the wrongful conduct alleged herein;
- whether Defendants owed a duty to Plaintiff and members of the Nationwide Class to adequately protect their personal information;
- whether Defendants breached their duties to protect the personal information of Plaintiff and Nationwide Class members;
- whether Defendants knew or should have known that its data security systems, policies, procedures, and practices were vulnerable;
- whether Plaintiff and Nationwide Class members suffered legally cognizable damages as a result of Defendants' conduct, including increased risk of identity theft and loss of value of PII/PHI;
- whether Defendants violated state consumer protection statutes; and
- whether Plaintiff and Nationwide Class members are entitled to equitable relief including injunctive relief.

69. **Typicality:** Plaintiff's claims are typical of the claims of the Nationwide Class members. Plaintiff, like all proposed Nationwide Class members, had their personal information compromised in the Data Breach.

70. **Adequacy:** Plaintiff will fairly and adequately protect the interests of the Nationwide Class. Plaintiff has no interests that are averse to, or in conflict with, the Nationwide Class members. There are no claims or defenses that are unique to Plaintiff. Likewise, Plaintiff has retained counsel experienced in class action and complex

litigation, including data breach litigation, and have sufficient resources to prosecute this action vigorously.

71. **Predominance:** The proposed action meets the requirements of Federal Rule of Civil Procedure 23(b)(3) because questions of law and fact common to the Nationwide Class predominate over any questions which may affect only individual Nationwide Class members.

72. **Superiority:** The proposed action also meets the requirements of Federal Rule of Civil Procedure 23(b)(3) because a class action is superior to other available methods for the fair and efficient adjudication of the controversy. Class treatment of common questions is superior to multiple individual actions or piecemeal litigation, avoids inconsistent decisions, presents far fewer management difficulties, conserves judicial resources and the parties' resources, and protects the rights of each class member.

73. Absent a class action, the majority Nationwide Class members would find the cost of litigating their claims prohibitively high and would have no effective remedy.

74. **Risks of Prosecuting Separate Actions:** Plaintiff's claims also meet the requirements of Federal Rule of Civil Procedure 23(b)(1) because prosecution of separate actions by individual class members would create a risk of inconsistent or varying adjudications that would establish incompatible standards for Defendants. Defendants continue to maintain the PII/PHI of Nationwide Class members and other individuals, and varying adjudications could establish incompatible standards with respect to its duty to protect individuals' personal information; and whether the injuries suffered by Nationwide Class members are legally cognizable, among others. Prosecution of separate action by individual class members would also create a risk of individual adjudications that would be dispositive of the interests of other class members not parties to the individual adjudications, or substantially impair or impede the ability of class members to protect their interests.

75. **Injunctive Relief:** In addition, Defendants have acted and/or refused to act on grounds that apply generally to the Nationwide Class, making injunctive and/or declaratory relief appropriate with respect to the class under Federal Rule of Civil Procedure 23(b)(2). Defendants continue to (1) maintain the personally identifiable information of Nationwide Class members, (2) fail to adequately protect their personally identifiable information, and (3) violate their rights under numerous state consumer protection laws and other claims alleged herein.

FIRST CAUSE OF ACTION

Negligence

(On Behalf of the Nationwide Class Against Defendants)

76. Plaintiff re-alleges and incorporates by reference all preceding factual allegations as though fully set forth herein.

77. Plaintiff brings this claim on behalf of herself and the Nationwide Class.

78. Plaintiff and Nationwide Class members were required to provide Defendants with their PII/PHI. Defendants collected and stored this information including their names, Social Security numbers, payment card information, checking account and routing numbers, insurance provider information, salary information, dates of birth, addresses, and phone numbers.

79. Defendants had a duty to Plaintiff and Nationwide Class members to safeguard and protect their PII/PHI.

80. Defendants assumed a duty of care to use reasonable means to secure and safeguard this PII/PHI, to prevent its disclosure, to guard it from theft, and to detect any attempted or actual breach of its systems.

81. Defendants have full knowledge about the sensitivity of Plaintiff and Nationwide Class members' PII/PHI, as well as the type of harm that would occur if such PII was wrongfully disclosed.

82. Defendants have a duty to use ordinary care in activities from which harm might be reasonably anticipated in connection with user PII/PHI data.

83. Defendants breached their duty of care by failing to secure and safeguard the PII of Plaintiff and Nationwide Class members. Defendants negligently stored and/or maintained its data security systems and published that information on the Internet.

84. Further, Defendants by and through their above negligent actions and/or inactions, breached their duties to Plaintiff and Nationwide Class members by failing to design, adopt, implement, control, manage, monitor and audit its processes, controls, policies, procedures and protocols for complying with the applicable laws and safeguarding and protecting Plaintiff's and Nationwide Class members' PII/PHI within their possession, custody and control.

85. Defendants further breached their duty to Plaintiff and Nationwide Class members by failing to comply with the California Confidentiality of Medical Information Act, Consumers Legal Remedies Act, the Customer Record's Act, the Gramm-Leach-Bliley Act, and other state and federal laws designed to protect Plaintiff and Class members from the type of harm they here have suffered. Such a breach by Defendants constitutes negligence per se.

86. Plaintiff and the other Nationwide Class members have suffered harm as a result of Defendants' negligence. These victims' loss of control over the compromised PII subjects each of them to a greatly enhanced risk of identity theft, fraud, and myriad other types of fraud and theft stemming from either use of the compromised information, or access to their user accounts.

87. It was reasonably foreseeable – in that Defendants knew or should have known – that its failure to exercise reasonable care in safeguarding and protecting Plaintiff's and Nationwide Class members' PII/PHI would result in its release and disclosure to unauthorized third parties who, in turn wrongfully used such PII/PHI, or disseminated it to other fraudsters for their wrongful use and for no lawful purpose.

88. But for Defendants' negligent and wrongful breach of their responsibilities and duties owed to Plaintiff and Nationwide Class members, their PII/PHI would not

have been compromised.

89. As a direct and proximate result of Defendants' above-described wrongful actions, inactions, and omissions, the resulting Data Breach, and the unauthorized release and disclosure of Plaintiff's and Nationwide Class members' PII/PHI, they have incurred (and will continue to incur) the above-referenced economic damages, and other actual injury and harm for which they are entitled to compensation. Defendants' wrongful actions, inactions, and omissions constituted (and continue to constitute) common law negligence/negligent misrepresentation.

90. Plaintiff and Nationwide Class members are entitled to injunctive relief as well as actual and punitive damages.

SECOND CAUSE OF ACTION

Violation of California Confidentiality of Medical Information Act, Cal. Civ. Code § 56, et seq.

(On Behalf of the Nationwide Class and California Sub-Class Against Defendants)

91. Plaintiff re-alleges and incorporates by reference all preceding factual allegations as though fully set forth herein.

92. California's Confidentiality of Medical Information Act ("CMIA") requires a healthcare provider "who creates, maintains, preserves, stores, abandons, destroys, or disposes of medical information [to] do so in a manner that preserves the confidentiality of the information contained therein." Cal. Civ. Code § 56.101. "Every provider of health care, health care service plan, pharmaceutical company, or contractor who negligently creates, maintains, preserves, stores, abandons, destroys, or disposes of medical information shall be subject to the remedies and penalties provided under subdivisions (b) and (c) of Section 56.36." *Id.*

93. The CMIA further requires that "[a]n electronic health record system or electronic medical record system . . . [p]rotect and preserve the integrity of electronic medical information." Cal. Civ. Code § 56.101(b)(1)(A).

94. Plaintiff, Nationwide Class members, and California Sub-Class members are "patient[s]," "whether or not still living, who received health care services from a provider of health care and to whom medical information pertains" pursuant to § 56.05(k) of the CMIA.

95. Quest Diagnostics is a "provider of healthcare" pursuant to § 56.05(m) of the CMIA "who creates, maintains, preserves, stores, abandons, destroys, or disposes of medical information."

96. Quest Diagnostics is subject to the requirements and mandates of the CMIA.

97. The PHI of Plaintiff, Nationwide Class members, and California Sub-Class members compromised in the Data Breach constitutes "medical information" maintained in electronic form pursuant to § 56.05(j) of the CMIA.

98. Defendants violated § 56.36(b) of the CMIA by negligently maintaining, preserving, storing and releasing the PHI of Plaintiff, Nationwide Class members, and California Sub-Class members, and failing to protect and preserve the integrity of the PHI of Plaintiff and California Subclass members.

99. Plaintiff, Nationwide Class members, and California Sub-Class members did not authorize Quest Diagnostics disclosure and release of their PHI that occurred in the Data Breach.

100. As a result of the Data Breach, the PHI of Plaintiff, Nationwide Class members, and California Sub-Class members was compromised when it was acquired and accessed by unauthorized parties.

101. Quest Diagnostics violated the CMIA by negligently (1) failing to implement reasonable administrative, physical and technical safeguards to protect, secure and prevent the unauthorized access to, and acquisition of, Plaintiff's and California Subclass members' PHI; (2) failing to implement reasonable data security measures, such as intrusion detection processes that detect data breaches in a timely manner, to protect and secure Plaintiff, Nationwide Class members, and California Sub-

Class members' PHI; (3) failing to use reasonable authentication procedures to track PHI in case of a security breach; and (4) allowing undetected and unauthorized access to servers, networks and systems where Plaintiff, Nationwide Class members, and California Sub-Class members' PHI was kept, all in violation of the CMIA.

102. Quest Diagnostics failure to implement adequate data security measures to protect the PHI of Plaintiff, Nationwide Class members, and California Sub-Class members was a substantial factor in allowing unauthorized parties to access Quest Diagnostics computer systems and acquire the PHI of Plaintiff and California Subclass members.

103. As a direct and proximate result of Quest Diagnostics violation of the CMIA, Quest Diagnostics allowed the PHI of Plaintiff, Nationwide Class members, and California Sub-Class members to: (a) escape and spread from its normal place of storage through unauthorized disclosure or release; and (b) be accessed and acquired by unauthorized parties in order to, on information and belief, view, mine, exploit, use, and/or profit from their PHI, thereby breaching the confidentiality of their PHI. Plaintiff and California Subclass members have accordingly sustained and will continue to sustain actual damages as set forth above.

104. Plaintiff, individually and on behalf of California Subclass members, seek actual and statutory damages pursuant to § 56.36(b)(1) of the CMIA.

105. Plaintiff also seek reasonable attorneys' fees and costs under applicable law including Federal Rule of Civil Procedure 23, Civil Code § 56.35, and California Code of Civil Procedure § 1021.5.

FOURTH CAUSE OF ACTION

N.Y. Gen. Bus. Law § 349

(On Behalf of the Nationwide Class Against Defendants)

106. Plaintiff realleges and incorporates by reference all preceding factual allegations.

107. Defendants, while operating in New York, engaged in deceptive acts and

practices in the conduct of business, trade and commerce, and the furnishing of services, in violation of N.Y. Gen. Bus. Law § 349(a). This includes but is not limited to the following:

a. Defendants failed to enact adequate privacy and security measures to protect the Class members' Sensitive from unauthorized disclosure, release, data breaches, and theft, which was a direct and proximate cause of the Data Breach;

b. Defendants failed to take proper action following known security risks and prior cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c. Defendants knowingly and fraudulently misrepresented that they would maintain adequate data privacy and security practices and procedures to safeguard the PII/PHI from unauthorized disclosure, release, data breaches, and theft;

d. Defendants omitted, suppressed, and concealed the material fact of Defendants' reliance on, and inadequacy of, AMCA's security protections;

e. Defendants knowingly and fraudulently misrepresented that they would comply with the requirements of relevant federal and state laws pertaining to the privacy and security of PII/PHI, including but not limited to duties imposed by HIPAA; and

f. Defendants failed to disclose the Data Breach to the victims in a timely and accurate manner, in violation of the duties imposed by, inter alia, N.Y. Gen Bus. Law § 899-aa(2).

108. As a direct and proximate result of Defendants' practices, Plaintiff and other Class Members suffered injury and/or damages, including but not limited to time and expenses related to monitoring their financial and medical accounts for fraudulent activity, an increased, imminent risk of fraud and identity theft, and loss of value of their PII/PHI.

109. The above unfair and deceptive acts and practices and acts by Defendants were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial

injury to Plaintiff and other Class members that they could not reasonably avoid, which outweighed any benefits to consumers or to competition.

110. Defendants knew or should have known that AMCA's computer systems and data security practices were inadequate to safeguard PII/PHI entrusted to it, and that risk of a data breach or theft was highly likely. Defendants' actions in engaging in the above-named unfair practices and deceptive acts were negligent, knowing and willful.

111. Plaintiff seeks relief under N.Y. Gen. Bus. Law § 349(h), including but not limited to actual damages (to be proven at trial), treble damages, statutory damages, injunctive relief, and/or attorney's fees and costs. The amount of such damages is to be determined at trial, but will not be less than $50.00 per violation. *Id.*

112. Plaintiff and Class Members seek to enjoin such unlawful deceptive acts and practices described above. Each Class Member will be irreparably harmed unless the Court enjoins Defendants' unlawful, deceptive actions in that Defendants will continue to fail to protect PII/PHI entrusted to them, as detailed herein.

113. Plaintiff and Class Members seek declaratory relief, restitution for monies wrongfully obtained, disgorgement of ill-gotten revenues and/or profits, injunctive relief prohibiting Defendant from continuing to disseminate its false and misleading statements, and other relief allowable under N.Y. Gen. Bus. Law § 349.

FOURTH CAUSE OF ACTION

Violation of California Consumers Legal Remedies Act, California Civil Code § 1750, *et seq.*

(On Behalf of the Nationwide Class and California Sub-Class Against Defendants)

114. Plaintiff re-alleges and incorporates by reference all preceding factual allegations as though fully set forth herein.

115. This cause of action is brought pursuant to the California Consumers Legal Remedies Act (the "CLRA"), California Civil Code § 1750, *et seq.* This cause of action does not seek monetary damages at this time but is limited solely to injunctive relief. Plaintiff will later amend this Complaint to seek damages in accordance with the CLRA

after providing Defendants with notice required by California Civil Code § 1782.

116. Plaintiff and Nationwide Class Members are "consumers," as the term is defined by California Civil Code § 1761(d).

117. Plaintiff, Nationwide Class members, and Defendants have engaged in "transactions," as that term is defined by California Civil Code § 1761(e).

118. The conduct alleged in this Complaint constitutes unfair methods of competition and unfair and deceptive acts and practices for the purpose of the CLRA, and the conduct was undertaken by Defendant was likely to deceive consumers.

119. Cal. Civ. Code § 1770(a)(5) prohibits one who is involved in a transaction from "[r]epresenting that goods or services have sponsorship, approval, characteristics, ingredients, uses, benefits, or quantities which they do not have."

120. Defendants violated this provision by representing that they took appropriate measures to protect Plaintiff's and the Nationwide Class members' PII/PHI. Additionally, Defendants improperly handled, stored, or protected either unencrypted or partially encrypted data.

121. As a result, Plaintiff and Nationwide Class members were induced to enter into a relationship with Defendants and provide their PII/PHI.

122. As a result of engaging in such conduct, Defendants have violated Civil Code § 1770.

123. Pursuant to Civil Code § 1780(a)(2) and (a)(5), Plaintiff seeks an order of this Court that includes, but is not limited to, an order enjoining Defendants from continuing to engage in unlawful, unfair, or fraudulent business practices or any other act prohibited by law.

124. Plaintiff and Nationwide Class members suffered injuries caused by Defendants' misrepresentations, because they provided their PII/PHI believing that Defendants would adequately protect this information.

125. Plaintiff and Nationwide Class members may be irreparably harmed and/or denied an effective and complete remedy if such an order is not granted.

126. The unfair and deceptive acts and practices of Defendants, as described above, present a serious threat to Plaintiff and members of the Nationwide Class.

FOURTH CAUSE OF ACTION

Violation of Unfair Competition Law,

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

(On Behalf of the Nationwide Class and California Sub-Class Against Defendants)

127. Plaintiff re-alleges and incorporates by reference all preceding factual allegations as though fully set forth herein.

128. Plaintiff brings this claim on behalf of herself and the Nationwide Class.

129. The California Unfair Competition Law, Cal. Bus. & Prof. Code §17200, *et seq*. ("UCL"), prohibits any "unlawful," "fraudulent" or "unfair" business act or practice and any false or misleading advertising, as defined by the UCL and relevant case law.

130. By reason of Defendants' above-described wrongful actions, inactions, and omissions, the resulting Data Breach, and the unauthorized disclosure of Plaintiff and Nationwide Class members' PII/PHI, Defendants engaged in unlawful, unfair and fraudulent practices within the meaning of the UCL.

131. Defendants' business practices as alleged herein are unfair because they offend established public policy and are immoral, unethical, oppressive, unscrupulous and substantially injurious to consumers, in that the private and confidential PII/PHI of consumers has been compromised for all to see, use, or otherwise exploit.

132. Defendants' practices were unlawful and in violation of Civil Code § 1798 *et seq*. because Defendants failed to take reasonable measures to protect Plaintiff's and the Nationwide Class members' PII/PHI.

133. Defendants' business practices as alleged herein are fraudulent because they are likely to deceive consumers into believing that the PII/PHI they provide to Defendants will remain private and secure, when in fact it was not private and secure.

134. Plaintiff and the Nationwide Class members suffered (and continue to

suffer) injury in fact and lost money or property as a direct and proximate result of Defendants' above-described wrongful actions, inactions, and omissions including, *inter alia*, the unauthorized release and disclosure of their PII/PHI.

135. Defendants' above-described wrongful actions, inactions, and omissions, the resulting Data Breach, and the unauthorized release and disclosure of Plaintiff's and Nationwide Class members' PII/PHI also constitute "unfair" business acts and practices within the meaning of Cal. Bus. & Prof. Code § 17200 *et seq*., in that Defendants' conduct was substantially injurious to Plaintiff and Nationwide Class members, offensive to public policy, immoral, unethical, oppressive and unscrupulous; the gravity of Defendants' conduct outweighs any alleged benefits attributable to such conduct.

136. But for Defendants' misrepresentations and omissions, Plaintiff and Nationwide Class members would not have provided their PII/PHI to Defendants or would have insisted that their PII/PHI be more securely protected.

137. As a direct and proximate result of Defendants' above-described wrongful actions, inactions, and omissions, the resulting Data Breach, and the unauthorized release and disclosure of Plaintiff and Nationwide Class members' PII/PHI, they have been injured: (1) the loss of the opportunity to control how their PII/PHI is used; (2) the diminution in the value and/or use of their PII/PHI entrusted to Defendants; (3) the compromise, publication, and/or theft of their PII/PHI; and (4) costs associated with monitoring their PII/PHI, amongst other things.

138. Plaintiff takes upon herself enforcement of the laws violated by Defendants in connection with the reckless and negligent disclosure of PII/PHI. There is a financial burden incurred in pursuing this action and it would be against the interests of justice to penalize Plaintiff by forcing him to pay attorneys' fees and costs from the recovery in this action. Therefore, an award of attorneys' fees and costs is appropriate under California Code of Civil Procedure § 1021.5.

///

///

FIFTH CAUSE OF ACTION

Violation of California Customer Records

Act, California Civil Code § 1798.80 et.seq.

(On Behalf of the Nationwide Class and California Sub-Class Against Defendants)

139. Plaintiff re-alleges and incorporates by reference all preceding factual allegations as though fully set forth herein.

140. "[T]o ensure that personal information about California residents is protected," Civil Code section 1798.81.5 requires that any business that "owns, licenses, or maintains personal information about a California resident shall implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure."

141. Defendants own, maintain, and license personal information, within the meaning of section 1798.81.5, about Plaintiff and the Nationwide Class.

142. Defendants violated Civil Code section 1798.81.5 by failing to implement reasonable measures to protect Plaintiff and Nationwide Class members' personal information.

143. As a direct and proximate result of Defendants' violations of section 1798.81.5 of the California Civil Code, the Data Breach described above occurred.

144. As a direct and proximate result of Defendants' violations of section 1798.81.5 of the California Civil Code, Plaintiff and the Nationwide Class members suffered the damages described above including, but not limited to, time and expenses related to monitoring their financial accounts for fraudulent activity, an increased, imminent risk of fraud and identity theft, and loss of value of their personally identifying information.

145. Plaintiff and the Nationwide Class members seek relief under section 1798.84 of the California Civil Code including, but not limited to, actual damages, to be proven at trial, and injunctive relief.

SIXTH CAUSE OF ACTION

Breach of Contract

(On Behalf of the Nationwide Class Against Defendants)

146. Plaintiff re-alleges the paragraphs above as if fully set forth herein.

147. Plaintiff and Class members entered into a contract with Defendants for the provision of title insurance or other closing services.

148. The terms of Defendants' privacy policy are part of the contract.

149. Plaintiff and Class members performed substantially all that was required of them under their contract with Defendants, or they were excused from doing so.

150. Defendants failed to perform its obligations under the contract, including by failing to provide adequate privacy, security, and confidentiality safeguards for Plaintiff and Class member's information and documents.

151. As a direct and proximate result of Defendants' breach of contract, Plaintiff and Class members did not receive the full benefit of the bargain, and instead received title insurance or other closing services that were less valuable than described in their contracts. Plaintiff and Class members, therefore, were damaged in an amount at least equal to the difference in value between that which was promised and Defendants' deficient performance.

152. Also, as a result of Defendants' breach of contract, Plaintiff and Class members have suffered actual damages resulting from the exposure of their personal information, and they remain at imminent risk of suffering additional damages in the future.

153. Accordingly, Plaintiff and Class members have been injured by Defendants' breach of contract and are entitled to damages and/or restitution in an amount to be proven at trial.

///

///

///

SEVENTH CAUSE OF ACTION

Breach of Implied Contract

(On Behalf of the Nationwide Class Against Defendants)

154. Plaintiff re-alleges the paragraphs above as if fully set forth herein.

155. Plaintiff brings this cause of action on behalf of the Class and to the extent necessary.

156. When Plaintiff and Class members paid money and provided their PII/PHI to Defendants in exchange for services, they entered into implied contracts with Defendants pursuant to which Defendants agreed to safeguard and protect such information and to timely and accurately notify them if their data had been breached and compromised.

157. Defendants solicited and invited prospective clients and other consumers to provide their PII/PHI as part of its regular business practices. These individuals accepted Defendants' offers and provided their PII/PHI to Defendants. In entering into such implied contracts, Plaintiff and the Class assumed that Defendants' data security practices and policies were reasonable and consistent with industry standards, and that Defendants would use part of the funds received from Plaintiff and the Class to pay for adequate and reasonable data security practices.

158. Plaintiff and the Class would not have provided and entrusted their PII/PHI to Defendants in the absence of the implied contract between them and Defendants to keep the information secure.

159. Plaintiff and the Class fully performed their obligations under the implied contracts with Defendants.

160. Defendants breached their implied contracts with Plaintiff and the Class by failing to safeguard and protect their PII/PHI and by failing to provide timely and accurate notice that their personal information was compromised as a result of a data breach.

161. As a direct and proximate result of Defendants' breaches of their implied

contracts, Plaintiff and the Class sustained actual losses and damages as described herein

EIGHTH CAUSE OF ACTION

Unjust Enrichment

(On Behalf of the Nationwide Class Against Defendants)

162. Plaintiff re-alleges the paragraphs above as if fully set forth herein.

163. Defendants received a benefit from Plaintiff and the Class in the form of payments for title insurance or other closing services.

164. The benefits received by Defendants were at Plaintiff's and the Class's expense.

165. The circumstances here are such that it would be unjust for Defendants to retain the portion of Plaintiff's and the Class's payments that should have been earmarked to provide adequate privacy, security, and confidentiality safeguards for Plaintiff and Class members' personal information and documents.

166. Plaintiff and the Class seek disgorgement of Defendants' ill-gotten gains.

NINTH CAUSE OF ACTION

Invasion of Privacy

(On Behalf of the Nationwide Class Against Defendants)

167. Plaintiff re-alleges the paragraphs above as if fully set forth herein.

168. Plaintiff brings this claim on behalf of himself and the Nationwide Class.

169. Plaintiff and Class members have a legally protected privacy interest in their PII/PHI that Defendants required them to provide and allow them to store.

170. Plaintiff and Class members reasonably expected that their PII/PHI would be protected and secured from unauthorized parties, would not be disclosed to any unauthorized parties or disclosed for any improper purpose.

171. Defendants unlawfully invaded the privacy rights of Plaintiff and Class members by (a) failing to adequately secure their PII/PHI from disclosure to unauthorized parties for improper purposes; (b) disclosing their PII/PHI to

unauthorized parties in a manner that is highly offensive to a reasonable person; and (c) disclosing their PII/PHI to unauthorized parties without the informed and clear consent of Plaintiff and Class members. This invasion into the privacy interest of Plaintiff and Class members is serious and substantial.

172. In failing to adequately secure Plaintiff's and Class members' PII/PHI, Defendants acted in reckless disregard of their privacy rights. Defendants knew or should have known that their substandard data security measures are highly offensive to a reasonable person in the same position as Plaintiff and Class members.

173. Defendants violated Plaintiff's and Class members' right to privacy under the common law as well as under state and federal law, including, but not limited to, the California Constitution, Article I, Section I.

174. As a direct and proximate result of Defendants' unlawful invasions of privacy, Plaintiff's and Class members' PII/PHI has been viewed or is at imminent risk of being viewed, and their reasonable expectations of privacy have been intruded upon and frustrated. Plaintiff and the proposed Class have suffered injury as a result of Defendants' unlawful invasions of privacy and are entitled to appropriate relief.

PRAYER FOR RELIEF

175. WHEREFORE, Plaintiff requests that the Court enter a judgment awarding the following relief:

a. An order certifying this action as a class action under Federal Rule of Civil Procedure 23, defining the Nationwide Class requested herein, appointing the undersigned as Class Counsel, and finding that Plaintiff is a proper representative of the Nationwide Class requested herein;

b. Injunctive relief requiring Defendants to (1) strengthen their data security systems that maintain personally identifying information to comply with the applicable state laws alleged herein (including, but not limited to, the California Customer Records Act) and best practices under industry standards; (2) engage third-party auditors and internal personnel to conduct security testing and audits on

Defendants' systems on a periodic basis; (3) promptly correct any problems or issues detected by such audits and testing; and (4) routinely and continually conduct training to inform internal security personnel how to prevent, identify and contain a breach, and how to appropriately respond;

c. An order requiring Defendant to pay all costs associated with class notice and administration of class-wide relief;

d. An award to Plaintiff and all Nationwide Class members of compensatory, consequential, incidental, and statutory damages, restitution, and disgorgement, in an amount to be determined at trial;

e. An award to Plaintiff and all Nationwide Class members credit monitoring and identity theft protection services;

f. An award of attorneys' fees, costs, and expenses, as provided by law or equity;

g. An order requiring Defendants to pay pre-judgment and post-judgment interest, as provided by law or equity; and

h. Such other or further relief as the Court may allow.

Dated: June 5, 2019

Respectfully submitted,

BISNAR|CHASE LLP

/s/ Jerusalem F. Beligan
BRIAN D. CHASE
JERUSALEM F. BELIGAN
IAN M. SILVERS

DEMAND FOR JURY TRIAL

Plaintiff demand a trial by jury of all issues in this action so triable of right.

Dated: June 5, 2019

Respectfully submitted,

BISNAR|CHASE LLP

/s/ Jerusalem F. Beligan
BRIAN D. CHASE
JERUSALEM F. BELIGAN
IAN M. SILVERS