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

IN THE UNITED STATES DISTRICT COURT

CENTRAL DISTRICT OF CALIFORNIA

BEN DINH, individually, and on behalf of all others similarly situated,

Plaintiff,

vs.

FIRST AMERICAN FINANCIAL CORPORATION; FIRST AMERICAN TITLE COMPANY; and DOES 1 through 10,

Defendants.

Case No.

CLASS ACTION COMPLAINT AND DEMAND FOR JURY TRIAL

Plaintiff Ben Dinh ("Plaintiff"), individually, and on behalf of the class defined below, brings this class action complaint against First American Financial Corporation, First American Title Company, and Does 1 through 10 (collectively, "First American" or "Defendants") and alleges as follows:

INTRODUCTION

1. On May 24, 2019, cybersecurity researcher Brian Krebs announced that First American published on its website more than 885 million sensitive mortgage documents (the "Data Breach"). These documents contained the confidential, private information of Plaintiff and putative Class members including, but not limited to, their names, email addresses, mailing addresses, dates of birth, social security numbers, bank account numbers, lender details, mortgage and tax records, driver's license images, and other personal information (collectively, "PII").

2. Since the Data Breach was first announced by Brian Krebs, First American has admitted that a design defect in one of its applications exposed the PII of its customers. Based on information and belief, First American hired an independent security forensic company and upon determining there was unauthorized access to Plaintiff and Class member's PII, First American shut down external access to the application.

3. While it is unclear when the Data Breach first began, the exposed documents date back to at least 2003 and were made available to the public without any security protection on the First American website. For instance, no username or password was required to view Plaintiff and Class members' PII, and the webpage lacked industry standard-two factor authentication.

4. Most disappointing is that First American allowed the Data Breach to occur, despite it being caused by a relatively common website design error called Insecure Direct Object Reference, which occurs when a link to a webpage with sensitive information is created and intended to only be seen by a specific party, but there is no method to actually verify the identity of who is viewing the link. As a result,

anyone who discovers a link to one document can view it—and can discover any of the other documents hosted on the site by simply modifying the link.

5. For instance, First American provided persons authorized to access specific documents by providing them with a URL to access the authorized documents on its website. That URL might end in "DocumentlD= 000000075."

6. Once that URL is obtained, anyone can access a different document which they are unauthorized to view by merely altering the numbers appearing at the end of the URL. For instance, by typing in the URL and ending it with "DocumentlD=000000076." If the numbers are further altered, additional documents that the person is not authorized to view will be revealed.

7. When announcing the Data Breach, Brian Krebs indicated that an identity thief could obtain all of the records through either "a low-and-slow or distributed indexing of this data [and it] would not have been difficult for even a novice attacker" to obtain. Moreover, websites, such as archive.org, have accessed and archived the records, thereby providing additional access of these records and further publishing them to the general public. Further, given the manner in which Defendants exposed the records, it is extremely likely web crawlers and/or spider bots have accessed and indexed these records making them available for identity thieves, no matter how Defendants responded to being informed of the Data Breach.

8. Armed with the PII from these records, hackers can sell the PII to other thieves or misuse them 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; or give false information to police during an arrest.

9. 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

10. Plaintiff Ben Dinh is a resident and citizen of Orange County, California. Plaintiff obtained a title search and purchased title insurance for his home in Westminster, California from First American. Through these services, Plaintiff provided Defendants his PII. As a result of Defendants' actions, Plaintiff 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 will need to purchase credit monitoring and take other measures to protect himself from identity theft and fraud. Plaintiff believed, at the time of obtaining a title search and purchasing title insurance, that First American would maintain the privacy and security of the documents he provided to it. Plaintiff further believes he paid a premium to First American for its data security. Plaintiff would not have used First American had he known that it would expose sensitive documents, making them publicly available over the internet.

11. Defendant First American Financial Corporation is a Delaware corporation with its principal place of business in Santa Ana, California.

12. Defendant First American Title Company is a California corporation with its principal place of business in Santa Ana, California. First American Title Company is a subsidiary of First American Financial Corporation.

13. The true names and/or capacities, whether individual, corporate, partnership, associate or otherwise, of the Defendants herein designated as Does and/or Roes 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 and/or Roes is negligently, willfully or otherwise legally responsible for the events and happenings herein referred to and proximately caused

damages to Plaintiffs 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.

14. Plaintiff is informed and believes and thereon alleges that at all times mentioned herein, Does and/or Roes 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

15. 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.

16. This Court may exercise personal jurisdiction over Defendants because they are registered to do business and have their principal places of business in California.

17. Venue is proper in this District under 28 U.S.C. § 1391 because Defendants are headquartered in this District, and a substantial part of the events or omissions giving rise to Plaintiff's claims occurred in this District.

FACTUAL ALLEGATIONS

A. The Data Breach

18. First American is the largest title insurance company in the United States, earning $5.3 billion per year in revenue from selling title insurance and other closing services. As Forbes noted in 2006, First American prices its title insurance

at 1,300% above its margin cost. The average policy with First American (in 2006) cost about $1,500 but running a title search—now that records are digitized—costs as little as $25. And First American pays only about $75 per policy to pay claims.

19. Customers believe that—at a minimum—the large sum they pay towards title insurance buys them security and peace of mind that their sensitive documents will be securely stored. As Ben Shoval, the man who discovered the First American breach, explains: "The title insurance agency collects all kinds of documents from both the buyer and seller, including Social Security numbers, driver's licenses, account statements ... You give them all kinds of private information and you expect that to stay private."

20. In its privacy policy, First American makes numerous promises to its customers that it will maintain the security and privacy of their personal information. For instance, First American states in its privacy policy that it is "Committed to Safeguarding Customer Information." Likewise, First American states in a section called "Confidentiality and Security," that it "will use our best efforts to ensure that no unauthorized parties have access to any of your information. We restrict access to nonpublic personal information about you to those individuals and entities who need to know that information . . . We currently maintain physical, electronic, and procedural safeguards that comply with federal regulations to guard your nonpublic personal information."

21. Additionally, First American ensures its customer it "will maintain appropriate . . . systems to protect against unauthorized access to . . . the data we maintain."

22. Meanwhile, First American claims the right to keep—indefinitely sensitive personal information for its own internal use: "We may, however, store such information indefinitely, including the period after which any customer relationship has ceased. Such information may be used for any internal purpose, such as quality control efforts or customer analysis."

23. By indefinitely storing sensitive documents on a publicly-accessible system, First American broke these privacy promises.

24. First American should know better, as it offers its own cybersecurity insurance product to companies in the event of "cyber security breaches, whether the result of cyber-attacks, cyber-crime, or internal carelessness."

25. Despite all of these promises, on May 24, 2019, a design defect on First American's website was announced by cybersecurity researcher Brian Krebs, whereby the personal, confidential records of Plaintiff and Class members were exposed and published on First American's website. The Data Breach exposed approximately 885 million sensitive mortgage documents, which contained Plaintiff and Class members PII, including, but not limited to, their names, email addresses, mailing addresses, dates of birth, social security numbers, bank account numbers, lender details, mortgage and tax records, driver's license images, and other personal information.

26. Brian Krebs learned about the Data Breach from a real estate developer, Ben Shoval. Although Mr. Shoval lacks a cybersecurity background, he quickly learned that he had access to, and did access, many documents he was not authorized to view. Although Mr. Shoval repeatedly reached out to First American to warn them of the Data Breach, he was ignored. First, he contacted First American's Chief Information Officer who did not respond. Then, Mr. Shoval contacted First American's Chief Executive Officer, who also ignored him. In a final attempt to stop the exposure, Mr. Shoval contacted cybersecurity researcher and journalist Brian Krebs, who finally confirmed that he had access.

27. Following reports of the Data Breach, First American provided the following statement:

> First American has learned of a design defect in an application that made possible unauthorized access to customer data. At First American, security, privacy and confidentiality are of the highest priority and we are committed to protecting our customers' information. The company took immediate action to address the

> situation and shut down external access to the application. We are currently evaluating what effect, if any, this had on the security of customer information. We will have no further comment until our internal review is completed.

28. While it is unclear when the Data Breach first began, the exposed documents appear to date back to 2003, and archive.org (a website that archives webpages on the Internet) shows documents available from the site dating back to at least March 2017.

29. As a result of Defendants' actions and omissions, these documents containing Plaintiff and Class members' PII were available to anyone with the document's URL, even if they were not authorized to review the document. Moreover, Defendants failed to require any username or password to accesses the documents and failed to implement numerous industry standard security features, such as two-factor authentication.

30. The Data Breach occurred because First American failed to prevent a relatively common website design error from occurring called Insecure Direct Object Reference, which occurs when a link to a webpage with sensitive information is created and intended to only be seen by a specific party, but there is no method to actually verify the identity of who is viewing the link. As a result, anyone who discovers a link to one document can view it—and can discover any of the other documents hosted on the site by simply modifying the link.

31. For instance, First American provided persons authorized to access specific documents by providing them with a URL to access the authorized documents on its website. That URL might end in "DocumentlD= 000000075."

32. Once that URL is obtained, anyone can access a different document which they are unauthorized to view by merely altering the numbers appearing at the end of the URL. For instance, by typing in the URL and ending it with "DocumentlD=000000076." If the numbers are further altered, additional documents that the person is not authorized to view will be revealed.

33. When announcing the Data Breach, Brian Krebs indicated that an

identity thief could obtain all of the records through either "a low-and-slow or distributed indexing of this data [and it] would not have been difficult for even a novice attacker" to obtain. Moreover, websites, such as archive.org, have accessed and archived the records, thereby providing additional access of these records and further publishing them to the general public. And, given the manner in which Defendants exposed the records, it is extremely likely web crawlers and/or spider bots have accessed and indexed these records making them available for identity thieves, no matter how Defendants responded to being informed of the Data Breach.

34. To date, First American has not yet provided a Notice of Data Breach and has not adequately explained how the Data Breach has occurred and why it took a third party to inform it of the Data Breach.

B. Personally Identifiable Information ("PII")

35. PII 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.

36. PII 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.

37. PII 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).

38. Given the nature of the Data Breach, it is foreseeable that the compromised PII will be used to access Plaintiff and the Class members' financial accounts, thereby providing access to additional PII or personal and sensitive information. Therefore, the compromised PII 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 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.

39. 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]

40. Names and dates of birth, combined with contact information like telephone numbers and email addresses, are very valuable to hackers and identity thieves as it allows them to access users' other accounts particularly when they have easily-decrypted passwords and security questions.

41. The PII First American 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.

42. Unfortunately for Plaintiff and Class members, a person whose PII has been compromised may not fully experience the effects of the breach for years

---

[1] 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 m n of Digital Privacy Controls (Dec. 2012) pp. 7-8.

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]

43. 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 is used without his or her permission to commit fraud or other crimes.[4]

44. 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]

45. To make matter worse, in 2017, the FBI warned the real estate industry of a "large spike in cyberattacks specifically targeting real estate companies." The FBI said that between 2016 and 2017, it witnessed a 480% increase in cyberattacks on the real estate industry.

46. First American ignored these warnings and risks and failed to invest in sufficient privacy and security protections.

47. One commentator noted that "even the most elementary PEN test"

---

[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].

would have found this data exposure. A PEN test, also called a penetration test, involves hiring a cybersecurity expert to look for and try to exploit vulnerabilities in the company's privacy and security configurations.

48. Another commentator noted that a routine "application security test" would have analyzed what information was exposed on the company's website to anonymous and regular users that shouldn't have been accessible to them.

49. As a direct and proximate result of First American's reckless and negligent actions, inaction, and omissions, the resulting Data Breach, the unauthorized release and disclosure of Plaintiff's and Class members' PII, and First American's 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 First American fails to undertake appropriate, legally required steps to protect the personal information in its possession.

50. 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]

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

CHOICE OF LAW ALLEGATIONS

52. The State of California has sufficient contacts regarding the conduct at issue in this Complaint, such that California law may be uniformly applied to the claims of the proposed Class.

53. Defendants do substantial business in California; their headquarters are located in California; and a significant portion of the proposed Nationwide Class is located in California.

54. In addition, the conduct that forms the basis for each and every Class member's claims against First American emanated from Defendants' headquarters in Santa Ana, California, where—among other things—Defendants stored customer information in its "cavernous data center"; Defendants set their privacy and compliance policies and practices; and Defendants planned their communications with Class members.

55. The State of California also has the greatest interest in applying its law to Class members' claims. California's governmental interests include not only compensating resident consumers under its consumer protection laws, but also what the State has characterized as a "compelling" interest in using its laws to regulate a resident corporation and preserve a business climate free of unfair and deceptive practices. *Diamond Multimedia Sys. v. Sup. Ct.*, 19 Cal. 4th 1036, 1064 (1999).

56. If other states' laws were applied to Class Members' claims,

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

California's interest in discouraging resident corporations from engaging in the sort of unfair and deceptive practices alleged in this complaint would be significantly impaired. California could not effectively regulate a company like First American, which does business throughout the United States, if it can only ensure remuneration for consumers from one of the fifty states affected by conduct that runs afoul of its laws.

CLASS ACTION ALLEGATIONS

57. 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

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

> *All persons who utilized First American's title insurance, title search, homeowner's insurance, mortgages, refinancing, home warranties, or other closing services provided by First American.*

59. Numerosity: The Nationwide Class is so numerous that joinder of all members is impracticable. Based on information and belief, the Nationwide Class includes millions of individuals from across the country who has their PII compromised, stolen, and published during the Data Breach. The parties will be able to identify the exact size of the class through discovery and First American's own documents.

60. 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;
- whether Defendants violated state consumer protection statutes; and
- whether Plaintiff and Nationwide Class members are entitled to equitable relief including injunctive relief.

61. **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.

62. **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.

63. **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.

64. **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.

65. 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.

66. 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 First American. First American continues to maintain the PII 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.

67. **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)

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

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

70. Plaintiff and Nationwide Class members were required to provide Defendants with their PII. 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.

71. Defendants had a duty to Plaintiff and Nationwide Class members to safeguard and protect their PII.

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

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

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

75. 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.

76. 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 within their possession, custody and control.

77. Defendants further breached their duty to Plaintiff and Nationwide Class members by failing to comply with the 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.

78. 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.

79. 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 would result in its release and disclosure to unauthorized third parties who, in turn wrongfully used such PII, or disseminated it to other fraudsters for their wrongful use and for no lawful purpose.

80. But for Defendants' negligent and wrongful breach of their responsibilities and duties owed to Plaintiff and Nationwide Class members, their PII would not have been compromised.

81. 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, 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.

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

SECOND CAUSE OF ACTION
Violation of California Consumers Legal Remedies Act, California Civil Code § 1750, *et seq.*
(On Behalf of the Nationwide Class Against Defendants)

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

84. 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.

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

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

87. 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.

88. 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."

89. Defendants violated this provision by representing that they took appropriate measures to protect Plaintiff's and the Nationwide Class members' PII.

Additionally, Defendants improperly handled, stored, or protected either unencrypted or partially encrypted data.

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

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

92. 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.

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

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

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

THIRD CAUSE OF ACTION

Violation of Unfair Competition Law, California Business and Professional Code Section 17200, *et seq*.

(On Behalf of the Nationwide Class Against Defendants)

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

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

98. 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.

99. 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, Defendants engaged in unlawful, unfair and fraudulent practices within the meaning of the UCL.

100. 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 of consumers has been compromised for all to see, use, or otherwise exploit.

101. 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.

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

103. 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.

104. 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 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.

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

106. 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, they have been injured: (1) the loss of the opportunity to control how their PII is used; (2) the diminution in the value and/or use of their PII entrusted to Defendants; (3) the compromise, publication, and/or theft of their PII; and (4) costs associated with monitoring their PII, amongst other things.

107. Plaintiff takes upon herself enforcement of the laws violated by Defendants in connection with the reckless and negligent disclosure of PII. 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.

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

109. "[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."

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

111. Defendants violated Civil Code section 1798.81.5 by failing to

implement reasonable measures to protect Plaintiff and Nationwide Class members' personal information.

112. 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.

113. 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.

114. 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.

FIFTH CAUSE OF ACTION
Breach of Contract
(On Behalf of the Nationwide Class Against Defendants)

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

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

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

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

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

120. 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.

121. 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.

122. 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.

SIXTH CAUSE OF ACTION
Unjust Enrichment
(On Behalf of the Nationwide Class Against Defendants)

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

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

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

126. 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 Plaintiffs and Class members' personal information and documents.

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

SEVENTH CAUSE OF ACTION
Invasion of Privacy
(On Behalf of the Nationwide Class Against Defendants)

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

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

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

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

132. Defendants unlawfully invaded the privacy rights of Plaintiffs and Class members by (a) failing to adequately secure their PII from disclosure to unauthorized parties for improper purposes; (b) disclosing their PII to unauthorized parties in a manner that is highly offensive to a reasonable person; and (c) disclosing their PII to unauthorized parties without the informed and clear consent of Plaintiffs and Class members. This invasion into the privacy interest of Plaintiff and Class members is serious and substantial.

133. In failing to adequately secure Plaintiff's and Class members' PII, 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.

134. 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.

135. As a direct and proximate result of Defendants' unlawful invasions of privacy, Plaintiff's and Class members' PII 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

136. 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 Defendants 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

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

Dated: June 4, 2019

Respectfully submitted,

BISNAR|CHASE LLP

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

DEMAND FOR JURY TRIAL

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

Dated: June 4, 2019

Respectfully submitted,

BISNAR|CHASE LLP

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