Jordan S. Esensten (SBN 264645)
jesensten@esenstenlaw.com
ESENSTEN LAW
12100 Wilshire Blvd., Suite 1660
Los Angeles, CA 90025
Telephone: (310) 273-3090
Facsimile: (310) 207-5969

Ivy T. Ngo (SBN 249860)
ivy@garner-associates.com
GARNER & ASSOCIATES LLP
520 Capitol Mall, Suite 280
Sacramento, CA 95814
Telephone: (530) 934-3324
Facsimile: (530) 934-2334

Interim Co-Lead Counsel for Plaintiffs and Putative Class

UNITED STATES DISTRICT COURT

CENTRAL DISTRICT OF CALIFORNIA

In Re First American Financial Corporation Cases	Case Nos. 8:19-cv-01105, 8:19-cv-01180, 8:19-cv-01305, 8:19-cv-01533 **CONSOLIDATED CLASS ACTION COMPLAINT FOR:** (1) Negligence (2) Breach of Contract (3) Breach of Implied Contract (4) Breach of Confidence (5) Violation of UCL, Cal. Bus. & Prof. Code §17200, *et seq.* (6) Violation of CLRA, Cal. Civ. Code §1750, *et seq.* (7) Deceit by Concealment, Cal. Civ. Code §§1709, 1710 (8) Violation of Customer Records Act, Cal. Civ. Code § 1798.80, *et seq.* (9) Violation of N.Y. Gen. Bus. Law § 349, *et seq.* **DEMAND FOR JURY TRIAL**

For their Consolidated Class Action Complaint ("Complaint"), Plaintiffs Ben Dinh ("Plaintiff Dinh"), Lasheeda Forney ("Plaintiff Forney"), Roger Campbell ("Plaintiff Campbell"), Gillian Schaadt ("Plaintiff Schaadt"), and Thaer Abdelrasoul ("Plaintiff Abdelrasoul") (collectively, "Plaintiffs"), on behalf of themselves and all others similarly situated, allege the following against Defendants First American Financial Corporation ("First American Financial") and First American Title Company ("First American Title") (collectively, "Defendants," "First American," or "the Company"), based on personal knowledge as to Plaintiffs and Plaintiffs' own acts, and on information and belief as to all other matters based upon, *inter alia*, the investigation conducted by and through Plaintiffs' undersigned counsel:

JURISDICTION AND VENUE

1. This Court has subject matter jurisdiction over this action pursuant to the Class Action Fairness Act ("CAFA"), 28 U.S.C. § 1332(d), because the aggregate amount in controversy exceeds $5,000,000, exclusive of interests and costs, there are more than 100 class members, and at least one class member is a citizen of a state different from Defendants.

2. This Court has personal jurisdiction over Defendants because Defendants regularly conduct business in California, are headquartered in Santa Ana, California, and accordingly have sufficient minimum contacts in California.

3. Venue is proper in this Court pursuant to 28 U.S.C. §§ 1391(a), (b) and/or (c) because Plaintiffs suffered injuries as a result of Defendants' acts in this District, a substantial number of the events giving rise to this Complaint occurred in this District, and Defendants are authorized to conduct business in this District and have intentionally availed themselves of the laws and markets of this District. Moreover, Defendants are headquartered in this District.

SUMMARY OF THE CASE

4. This case arises out of Defendants' failure to adequately safeguard

Plaintiffs' and the other Class members' valuable and sensitive personally identifiable information, 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 highly sensitive personal information (collectively, "PII"), resulting in First American publishing on its web-based document delivery system more than 885 million documents exposing Plaintiffs' and the other Class members' PII to unauthorized users (the "Data Breach").

5. Plaintiffs and the other Class members provided Defendants with their PII when they applied for and/or purchased title insurance, home warranties, and/or other real estate transaction closing services provided by Defendants.

6. When Plaintiffs and the other Class members submitted documents to Defendants, Defendants provided them with a URL to access their documents on Defendants' web-based document delivery system. Each document containing PII was assigned a specific numerical designation reflected in the URL, such as "DocumentID=000000121."

7. Because Defendants' web-based document delivery system lacked even the most rudimentary security measures, anyone with a valid URL could alter the "DocumentID=" number in the URL to access other documents. For example, entering "DocumentID=000000122" would provide access to the document corresponding to that "DocumentID," regardless of whether the person accessing that document was authorized to do so. That same person could thereafter enter a URL with "DocumentID=000000123" and be provided with unauthorized access to the corresponding document.

8. On May 24, 2019, cybersecurity researcher Brian Krebs announced that all 885 million documents available on Defendants' server were accessible via the Internet using this simple number swap because all of the "DocumentID" numbers were sequential.

9. 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 Defendants' web-based document delivery system.

10. When announcing the Data Breach, Brian Krebs indicated that an identity thief could obtain all of the documents 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 documents, thereby providing additional access to these documents and further publishing of them to the general public. Given the manner in which Defendants exposed Plaintiffs' and Class members' PII and documents, it is extremely likely web crawlers and/or spider bots have accessed and indexed these documents making them available for identity thieves, no matter how Defendants responded after being informed of the Data Breach.

11. After the Data Breach was first announced, but not before allowing unauthorized access to Plaintiffs' and Class members' sensitive PII and documents, Defendants have admitted that a design defect in one of its applications exposed the PII of its customers. Based on information and belief, Defendants hired an independent security forensic company and, upon determining there was unauthorized access to Plaintiffs' and the other Class members' PII, shut down external access to the application.

12. Nevertheless, Defendants have yet to directly inform or notify Plaintiffs and all of the Class members that their PII may be compromised as a result of the Data Breach.

13. Defendants failed to maintain adequate security measures occurred despite their representations and promises to Plaintiffs and the other Class members that their PII would be safeguarded.

14. The sophisticated and highly sensitive nature of the PII contained in Plaintiffs' and the other Class Members' documents virtually guarantees that the

PII will be used in future acts of cyber-fraud and identity theft. These future acts of fraud or identity theft could be perpetrated by the hackers themselves or sold on the dark web to other malicious actors.

15. As a result of Defendants' failure to maintain adequate security measures, Plaintiffs' and the other Class members' PII, including social security numbers, addresses, dates of birth, banking information, and more, was compromised. In order to mitigate the increased risk of future harm, Plaintiffs and the other Class members are left with the undesirable tasks of undertaking additional security measures, at their own expense, by, without limitation, closing credit card accounts, bank accounts, debit card accounts, etc. But there is no guarantee that such security measures will in fact adequately protect their PII.

PARTIES

16. Plaintiff Dinh is, and was at all relevant times, a resident of the State of California. In 2019, Plaintiff Dinh obtained a title search and purchased title insurance for a house in Westminster, California from First American. Through these services, Plaintiff Dinh provided Defendants his PII. At the time of transaction, Plaintiff Dinh believed that First American would maintain the privacy and security of the documents he provided to First American. Plaintiff Dinh would not have used First American's services had he known that it employed inadequate security measures for protecting his PII or that it would expose his sensitive information, making it publicly available over the internet. As a result of Defendants' actions or inactions, Plaintiff Dinh has been injured because the First American Data Breach has placed him at substantial risk of identity theft or fraud including, but not limited to, credit card fraud, phone or utilities fraud, bank fraud and government fraud. As a further result of Defendants' actions, Plaintiff Dinh has spent, and continues to spend, considerable time and effort proactively taking measures to protect himself and his accounts from identity theft or fraud.

17. Plaintiff Forney is, and was at all relevant times, a resident of the State

of California. In 2013, Plaintiff Forney purchased a home and First American Home Warranty. Plaintiff Forney filled out and submitted the warranty application in Sacramento, California. In connection with the purchase, Plaintiff Forney provided Defendants with her PII. At the time of transaction, Plaintiff Forney believed that First American would maintain the privacy and security of the documents she provided to First American. Plaintiff Forney would not have used First American's services had she known that it employed inadequate security measures for protecting her PII or that it would expose her sensitive information, making it publicly available over the internet. As a result of Defendants' actions or inactions, Plaintiff Forney has been injured by, among other things, having to spend considerable time and effort dealing with a tax return fraudulently filed in her name in January 2017 and credit cards fraudulently opened in her name in early 2017. She incurred late fees on her bills in February-May 2017 because she received her 2017 tax refund approximately three months late and she has incurred and is still incurring legal fees because she hired a law firm to help her with the identify theft. In addition, her credit score has dropped over 200 points because of the fraudulently opened credit cards, impacting her ability to obtain financing for a house or car, and has only minimally recovered because the fraudulently opened credit cards are still on her credit report. The First American Data Breach has placed her at substantial risk of additional identity theft or fraud including, but not limited to, credit card fraud, phone or utilities fraud, bank fraud and government fraud. As a further result of Defendants' actions or inactions, Plaintiff Forney will need to purchase credit monitoring and take other measures to protect herself from identity theft and fraud. Plaintiff Forney is not aware of her PII being exposed and/or impacted by any other data breaches.

18. Plaintiff Campbell is, and was at all relevant times, a resident of the State of California. In 2018, Plaintiff Campbell obtained a title search and purchased title insurance for a house in Copperopolis, California from First American.

Through these services, Plaintiff Campbell provided Defendants his PII. At the time of transaction, Plaintiff Campbell believed that First American would maintain the privacy and security of the documents he provided to First American. Plaintiff Campbell would not have used First American's services had he known that it employed inadequate security measures for protecting his PII. Plaintiff Campbell would not have used First American's services had he known that it would expose his sensitive information, making it publicly available over the internet. As a result of Defendants' actions or inactions, Plaintiff Campbell has been injured, by among other things, having to spend considerable time and effort dealing with fraudulent charges on his debit card and multiple of his credit cards totaling approximately $1800. In addition, his credit score has dropped approximately 90 points and has only recovered about 50%, which prevented him from installing solar panels and caused him to have a higher interest rate when he attempted to buy a car. The First American Data Breach has placed him at substantial risk of additional identity theft or fraud including, but not limited to, credit card fraud, phone or utilities fraud, bank fraud and government fraud. As a further result of Defendants' actions or inactions, Plaintiff Campbell will need to purchase credit monitoring and take other measures to protect himself from identity theft and fraud. Plaintiff Campbell is not aware of his PII being exposed and/or impacted by any other data breaches.

19. Plaintiff Schaadt is, and was at all relevant times, a resident of the State of California. In 2012 and 2016, Plaintiff Schaadt obtained a title search and purchased title insurance for houses in Ladera Ranch, California from First American. Through these services, Plaintiff Schaadt provided Defendants her PII. At the time of transaction, Plaintiff Schaadt believed that First American would maintain the privacy and security of the documents she provided to First American. Plaintiff Schaadt would not have used First American's services had she known that it employed inadequate security measures for protecting her PII or that it would expose her sensitive information, making it publicly available over the internet. As

a result of Defendants' actions or inactions, Plaintiff Schaadt has been injured by, among other things, having to spend considerable time and effort dealing with a fraudulently created identification card by a woman who then withdrew money from Plaintiff Schaadt's account in May 2019. Not only has Plaintiff Schaadt taken approximately two weeks off of work to deal with this identify theft and gone to the trouble of filing a police report, she has had to put fraud alerts and change all her security information on all her personal accounts and freeze and unfreeze her credit as needed. The First American Data Breach has placed her at substantial risk of additional identity theft or fraud including, but not limited to, credit card fraud, phone or utilities fraud, bank fraud and government fraud. As a further result of Defendants' actions or inactions, Plaintiff Schaadt will need to purchase credit monitoring and take other measures to protect herself from identity theft and fraud. Plaintiff Schaadt is not aware of her PII being exposed and/or impacted by any other data breaches.

20. Plaintiff Abdelrasoul is, and was at all relevant times, a resident of the State of New York. On April 10, 2019, Plaintiff Abdelrasoul obtained a title search and purchased title insurance for a house in Staten Island, New York from First American. Through these services, Plaintiff Abdelrasoul provided Defendants his PII. At the time of transaction, Plaintiff Abdelrasoul believed that First American would maintain the privacy and security of the documents he provided to First American. Plaintiff Abdelrasoul would not have used First American's services had he known that it employed inadequate security measures for protecting his PII. Plaintiff Abdelrasoul would not have used First American's services had he known that it would expose his sensitive information, making it publicly available over the internet. As a result of Defendants' actions or inactions, Plaintiff Abdelrasoul has been injured because the First American Data Breach has placed him at substantial risk of identity theft or fraud including, but not limited to, credit card fraud, phone or utilities fraud, bank fraud and government fraud. As a further result of

Defendants' actions or inactions, Plaintiff Abdelrasoul has spent, and continues to spend, considerable time and effort proactively taking measures to protect himself and his accounts from identity theft or fraud and dealing with phishing emails and phone calls.

21. First American Financial is a Delaware corporation with its headquarters located in the State of California and conducts a significant portion of its business across the United States.

22. First American Title is a California corporation, with its headquarters in the State of California, and is a subsidiary of First American Financial.

FACTUAL ALLEGATIONS

A. First American and its Promise to Customers

23. First American is the second largest provider of title insurance in the United States.[1] First American earned over $5.7 billion in revenue during the past two years, and "[a] substantial portion of the revenues for [First American's] title insurance and services segment results from the sale and refinancing of residential and commercial real estate."[2]

24. Essentially mandatory for obtaining a mortgage, title insurance is extraordinarily expensive. 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) costs about $1,500, but running a title search—now that records are digitized—costs as little as $25.16. And, First American pays only about $75 per policy to pay claims.[3]

25. Customers believe that—at a minimum—the large sum they pay

[1] First American Financial Corporation 2018 Annual Report, *available at* http://s21.q4cdn.com/992793803/files/doc_financials/2018/Annual/2018-FAF-Annual-Report.pdf (last visited April 20, 2020).

[2] *Id.*

[3] Scott Woolley, *Inside America's Richest Insurance Racket*, Forbes (Oct. 28, 2006), *available at* https://www.forbes.com/forbes/2006/1113/148 (last visited April 20, 2020).

towards title insurance buys them security and peace of mind that their sensitive documents will be securely stored. As Ben Shoval, a real estate developer and the person 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, drivers licenses, account statements …. You give them all kinds of private information and you expect that to stay private.'"[4]

26. First American assures prospective customers that it is "equipped with the necessary tools to provide a complete document management program aimed at mitigating risk."[5] As one of the "Benefits of Our Services," First American lists: "Secure access to files."[6] Under "Secure Document Storage," First American promises to provide "secure, reliable, and affordable records storage solutions."[7]

27. First American's policy on Privacy Information is also littered with numerous promises to its customers that First American will maintain the security and privacy of their personal information ("Privacy Policy"). The very first sentence of First American's Privacy Policy reads: "We Are Committed to Safeguarding Customer Information."[8] In a later section on "Confidentiality and Security," First American states: "We will use our best efforts to ensure that no unauthorized parties have access to any of your information."[9] It goes on to state that First American "restrict[s] access to nonpublic personal information about you to those individuals

[4] Brian Krebs, *First American Financial Corp. Leaked Hundreds of Millions of Title Insurance Records*, KrebsOnSecurity *available at* https://krebsonsecurity.com/2019/05/first-american-financial-corp-leaked-hundreds-of-millions-of-title-insurance-records/ (last visited April 20, 2020).

[5] https://www.firstam.com/mortgagesolutions/solutions/cleanfile-solutions/document-management.html (last visited April 20, 2020).

[6] https://www.firstam.com/mortgagesolutions/solutions/foreclosure-reo/asset-closing-services.html (last visited April 20, 2020).

[7] https://www.firstam.com/mortgagesolutions/solutions/cleanfile-solutions/document-management.html (last visited April 20, 2020).

[8] First American Privacy Information, *available at* http://web.archive.org/web/20190525235150/https:/www.firstam.com/privacy-policy/index.html (last visited April 20, 2020).

[9] *Id.*

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."[10] Ultimately, First American's Privacy Policy promises customers that "We will maintain appropriate … systems to protect against unauthorized access to … the data we maintain."[11]

28. Meanwhile, First American claims the right to keep—indefinitely—sensitive PII 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."[12]

B. The Data Breach

29. Despite these promises, assurances, and representations, First American's document storage solutions were anything but secure. On May 24, 2019, cybersecurity guru Brian Krebs announced that 885 million files were exposed on First American's web-based document delivery system for anyone with a valid URL for a single document to access.[13] The files contained bank account numbers, social security numbers, financial and tax records, and images of driver's licenses.

30. Brian Krebs learned about the Data Breach from a real estate developer, Ben Shoval.[14] Although Mr. Shoval lacks a cybersecurity background, he quickly learned that he had access to, and did access, many documents containing PII he was not authorized to access or view.[15] Mr. Shoval repeatedly reached out to

---

[10] *Id.*

[11] *Id.*

[12] *Id.*

[13] *First American Financial Corp. Leaked Hundreds of Millions of Title Insurance Records*, *supra* fn. 4

[14] *Id.*

[15] *Id.*

First American to warn it of the problem, but was ignored. Mr. Shoval contacted First American's Chief Information Officer who did not respond. Mr. Shoval then contacted First American's Chief Executive Officer, who also ignored him. Mr. Shoval then contacted cybersecurity researcher and journalist Brian Krebs, who confirmed that he had access. When Mr. Krebs reached out to First American, he too was ignored.

31. Following public reports of the Data Breach, First American finally took action and 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.

32. 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 date back to at least March 2017.

33. The Data Breach occurred because First American failed to prevent a relatively basic 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 URL. As a result, once a URL is obtained, anyone can access a different document by merely altering the numbers appearing at the end, regardless of whether they are authorized to view such documents. The design error is so basic that seeing the "DocumentID=[number]" at the end of the URL is practically an invitation for data thieves, lay persons, and persons with and without cybersecurity credentials, to act on their curiosity and test

the web-based document delivery system's security measures.

34. First American should have known of its own vulnerabilities, and should have, at the very least, investigated the adequacy of its security measures, particularly when between 2016 and 2017, there was a 480% increase in cyberattacks on the real estate industry.[16]

35. Had First American not ignored the fact that the real estate industry was experiencing a substantial uptick in cyberattacks, it would have discovered its own vulnerabilities and could have avoided exposing Plaintiffs' and the other Class members' PII in the Data Breach. Cybersecurity researcher Brian Krebs says that mass-harvesting the 885 million records from First American's web-based document delivery system "would not have been difficult for even a novice attacker."[17] Mr. Krebs also notes that "the information exposed by First American would be a virtual gold mine for phishers and scammers."[18]

36. According to FBI data, the costliest form of cybercrimes are ones that "often impersonate real estate agents, closing agencies, title and escrow firms in a bid to trick property buyers into wiring funds to fraudsters."[19] The documents leaked by First American contain not only sensitive information that scammers can use to impersonate real estate sellers, but also contact information for specific closing agents and buyers involved in ongoing real estate transactions.

37. By indefinitely storing sensitive documents on a publicly-accessible system, First American broke its privacy promises to its customers.

38. First American should know better, as it offers its own cybersecurity

---

[16] *Real Estate Security is More Important Than Ever: 3 Ways To Brace Your Team Against Cybercrime*, Auth0, *available at* https://web.archive.org/web/20190526031109/https:/auth0.com/blog/amp/cybersecurity-and-cybercrime-in-real-estate-industry/

[17] *First American Financial Corp. Leaked Hundreds of Millions of Title Insurance Records*, *supra* fn. 4.

[18] *Id.*

[19] *Id.*

insurance product to companies in the event of "cyber security breaches, whether the result of cyber-attacks, cyber-crime, or internal carelessness."[20]

39. Based on information and belief, Plaintiffs allege that to date, First American has yet to provide a Notice of Data Breach to Plaintiffs or all of the Class members and has not adequately explained how the Data Breach occurred, why First American's internal processes did not detect the design flaw, why third parties without cybersecurity credentials were able to access the PII, or why the warnings of third parties went ignored.

C. The Value of PII

40. 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.

41. The types of information compromised in the Data Breach are highly valuable to cybercriminals. Bank account numbers, social security numbers, financial and tax records, and images of driver's licenses can all be used to defraud First American customers of money and property.

42. Given the nature of the Data Breach, it is foreseeable that the compromised PII could be used to access Plaintiffs and the other Class members' financial accounts, thereby providing access to additional PII or personal and sensitive information.

43. Identity thieves can also use the PII to harm Plaintiffs and the other Class members through embarrassment, blackmail, or harassment in person or online, or to commit other types of fraud including obtaining ID cards or driver's licenses, fraudulently obtaining tax returns and refunds, and obtaining government

[20] https://www.firstam.com/title/agency/agency-insurance/ (last visited April 20, 2020).

benefits. A Presidential Report on identity theft from 2008 states that:

> In addition to the losses that result when identity thieves fraudulently open accounts or misuse existing accounts, . . . individual victims often suffer indirect financial costs, including the costs incurred in both civil litigation initiated by creditors and in overcoming the many obstacles they face in obtaining or retaining credit. Victims of non-financial identity theft, for example, health-related or criminal record fraud, face other types of harm and frustration.
>
> In addition to out-of-pocket expenses that can reach thousands of dollars for the victims of new account identity theft, and the emotional toll identity theft can take, some victims have to spend what can be a considerable amount of time to repair the damage caused by the identity thieves. Victims of new account identity theft, for example, must correct fraudulent information in their credit reports and monitor their reports for future inaccuracies, close existing bank accounts and open new ones, and dispute charges with individual creditors.[21]

44. To put it into context, the 2013 Norton report – based on one of the largest consumer cybercrime studies ever conducted – estimated that the global price tag of cybercrime was around $113 billion at that time, with the average cost per victim being $298 dollars.[22] That number no doubt increased after the PII of Plaintiffs and the other Class members was leaked in the Data Breach.

45. The problems associated with identity theft are exacerbated by the fact that many cybercriminals will wait years before attempting to use the PII they have obtained. Indeed, in order to protect themselves, Plaintiffs and the other Class members will need to remain vigilant against unauthorized data use for years and decades to come.

46. Once stolen, PII can be used in a number of different ways. One of the most common ways is that it is offered for sale on the "dark web," a heavily encrypted part of the Internet that makes it difficult for authorities to detect the

[21] *The President's Identity Theft Task Force, Combating Identity Theft: A Strategic Plan*, Federal Trade Commission, (April 2007), *available at* http://www.ftc.gov/sites/default/files/documents/reports/combating-identity-theft-strategic-plan/strategicplan.pdf (last visited April 20, 2020).

[22] Norton by Symantec, *2013 Norton Report*, *available at* https://yle.fi/tvuutiset/uutiset/upics/liitetiedostot/norton_raportti.pdf (last visited April 20, 2020).

location or owners of a website. The dark web is not indexed by normal search engines such as Google and is only accessible using a Tor browser (or similar tool) which aims to conceal users' identities and online activity. The dark web is notorious for hosting marketplaces selling illegal items such as weapons, drugs, and PII.[23] Websites appear and disappear quickly, making it a very dynamic environment.

47. Due to its concealed and sometimes disguised nature, coupled with the intentional use of special applications to maintain anonymity, the dark web is a haven for a plethora of illicit activity, including the trafficking of stolen PII captured via data breaches or hacks.[24] One 2018 study found that an individual's online identity is worth as much as approximately $1,170 on the dark web.[25]

48. Once someone buys PII, it is then used to gain access to different areas of the victim's digital life, including bank accounts, social media, and credit card details. During that process, other sensitive data may be harvested from the victim's accounts, as well as from those belonging to family, friends, and colleagues.

49. PII can also be used by cybercriminals to target victims using phishing scams.[26] Phishing is when scammers use personal information they have obtained about victims to send fraudulent emails, texts, or copycat websites to get victims to share additional valuable personal information – such as login IDs and passwords.[27]

---

[23] Brian Hamrick, *The dark web: A trip into the underbelly of the internet*, *available at* https://www.wlwt.com/article/the-dark-web-a-trip-into-the-underbelly-of-the-internet/8698419 (last visited April 20, 2020).

[24] Ellen Sirull, *What is the Dark Web?*, Experian, Apr. 8, 2018, https://www.experian.com/blogs/ask-experian/what-is-the-dark-web/; *see also The dark web: A trip into the underbelly of the internet*, *supra.* fn. 34.

[25] Simon Migliano, Dark Web Market Place Index (US Edition), TOP10VPN, Feb. 28, 2018, https://www.top10vpn.com/privacy-central/privacy/dark-web-market-price-index-feb-2018-us/ (last visited April 20, 2020).

[26] *How to Recognize and Avoid Phishing Scams*, U.S. Federal Trade Commission, May 2019, https://www.consumer.ftc.gov/articles/how-recognize-and-avoid-phishing-scams (last visited April 20, 2020).

[27] *Id.*

Scammers also use phishing emails to get access to a victim's compute or network, then install programs like ransomware that can lock a victim out of important files on their computer.[28] According to one Federal Bureau of Investigation study, scammers collected more than $676 million in 2017 alone through two types of phishing scams: "Business Email Compromise" and "Email Account Compromise."[29]

50. In 2017, the FBI warned the real estate industry of a "large spike in cyberattacks specifically targeting real estate companies."[30] The FBI said that between 2016 and 2017, there had been a 480% increase in cyberattacks on the real estate industry.[31]

51. As authentication provider Auth0 notes, "Real estate tech is also one of the fastest growing tech sectors. High-value areas often draw criminals."[32]

52. First American ignored these warnings and failed to invest in sufficient security measures.

53. One commenter noted that with regard to the First American Data Breach, "even the most elementary PEN test" would have found this data exposure.[33] 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.

54. Another commenter noted that a routine "application security test"

---

[28] *Id.*

[29] *2017 Internet Crime Report*, U.S. Federal Bureau of Investigation, https://pdf.ic3.gov/2017_IC3Report.pdf (last visited April 20, 2020).

[30] *Real Estate Security is More Important Than Ever: 3 Ways To Brace Your Team Against Cybercrime*, Auth0, *available at* https://web.archive.org/web/20190526031109/https:/auth0.com/blog/amp/cybersecurity-and-cybercrime-in-real-estate-industry/ (last visited April 20, 2020).

[31] *Id.*

[32] *Id.*

[33] *First American Financial Corp. Leaked Hundreds of Millions of Title Insurance Records*, *supra* fn. 6.

would have analyzed what information was exposed on First America's web-based document delivery system to anonymous and regular users that should not have been accessible to them.[34]

55. The failure to conduct sufficient application security testing may be due—in part—to First American's decision to appoint someone whom it hired as an administrative assistant to be the "Head of Enterprise Application Security."[35]

56. The Data Breach and exposure of the PII has immediately, directly and substantially increased Plaintiffs and the other Class members' risk of identity theft. As a result of the Data Breach, Plaintiffs and the other Class members have also suffered nuisance and a loss of privacy, and must now expend additional time and money mitigating the threat of identity theft, which would not have ben necessary but for the Data Breach.

57. The insufficient security policies and procedures implemented by First American are a material fact that a reasonable consumer would take into consideration when deciding whether to provide Defendants with personal and confidential information. Had Plaintiffs and the other Class members known that Defendants failed to employ necessary and adequate protection of their PII, they would not have used First American or would have otherwise limited the PII shared with Defendants.

CHOICE OF LAW ALLEGATIONS

58. 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.

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

[34] *Id.*

[35] *See* https://www.linkedin.com/in/diana-esparza-5377273/ (last visited April 20, 2020).

located in California.

60. The conduct that forms the basis of 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.

61. 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. Superior Court*, 19 Cal. 4th 1036, 1064 (1999).

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

63. Pursuant to Rules 23(b)(1), (b)(2), (b)(3), and (c)(4) of the Federal Rules of Civil Procedure, Plaintiffs, individually and on behalf of all others similarly situated, bring this lawsuit on behalf of themselves and as a class action on behalf of the following Class and Sub-Class:

> **Nationwide Class**: All persons in the United States who provided documents containing PII to First American whose information was

exposed, accessed, compromised or stolen in the Data Breach.

California Sub-Class: All California residents who provided documents containing PII to First American whose information was exposed, accessed, compromised or stolen in the Data Breach.

New York Sub-Class: All New York residents who provided documents containing PII to First American whose information was exposed, accessed, compromised or stolen in the Data Breach.

64. Excluded from the Class are Defendants and any entities in which Defendants or their subsidiaries or affiliates have a controlling interest, and Defendants' officers, agents, and employees. Also excluded from the Class is any judge assigned to this action, members of the judge's staff, and any member of the judge's immediate family. Plaintiffs reserve the right to amend the Class definition if discovery and further investigation reveal that it should be expanded or otherwise modified.

65. **Numerosity**: The members of the Class are so numerous that joinder of all members of the Class would be impracticable. Plaintiffs reasonably believe that Class members number hundreds of millions of people or more in the aggregate and well over 1,000. The names and addresses of Class members are identifiable through documents maintained by Defendants. Notice can be provided to Class members through direct mailing, publication, or otherwise using techniques and a form of notice similar to those customarily used in class actions arising under state and federal law.

66. **Commonality and Predominance**: This action involves common questions of law or fact, which predominate over any questions affecting individual Class members, including:

a. Whether Defendants failed to maintain adequate security measures;

b. Whether Defendants were contractually obligated to provide Plaintiffs and the other Class members with adequate security measures;

c. Whether Defendants breached their contractual obligations to Plaintiffs and the other Class members.

d. Whether Defendants represented to Class members that they would safeguard Plaintiffs' and the other Class members' PII;

e. Whether Defendants owed a legal duty to Plaintiffs and the other Class members to exercise due care in collecting, storing, and safeguarding their PII;

f. Whether Defendants breached a legal duty to Plaintiffs and the other Class members to exercise due care in collecting, storing, and safeguarding their PII;

g. Whether Plaintiffs' and the other Class members' PII was accessed, compromised, or stolen in the Data Breach;

h. Whether Plaintiffs and the other Class members are entitled to equitable relief including, but not limited to, injunctive relief and restitution; and

i. Whether Plaintiffs and the other Class members are entitled to actual, statutory, or other forms of damages, and other monetary relief.

67. Similar or identical statutory and common law violations, business practices, and injuries are involved. Individual questions, if any, pale by comparison, in both quantity and quality, to the numerous common questions that dominate this action.

68. **Typicality**: Plaintiffs' claims are typical of the claims of the other members of the Class because, among other things, Plaintiffs and the other Class members were injured through the substantially uniform misconduct of Defendants. Plaintiffs are advancing the same claims and legal theories on behalf of themselves and all other Class members, and there are no defenses that are unique to Plaintiffs. The claims of Plaintiffs and of all other Class members arise from the same operative facts and are based on the same legal theories.

69. **Adequacy of Representation**: Plaintiffs are adequate representatives of the Class because their interests do not conflict with the interests of the other

Class members they seek to represent; they have retained counsel competent and experienced in complex class action litigation; and they will prosecute this action vigorously. The Class members' interests will be fairly and adequately protected by Plaintiffs and their counsel.

70. **Superiority**: A class action is superior to any other available means for the fair and efficient adjudication of this controversy, and no unusual difficulties are likely to be encountered in the management of this matter as a class action. The damages, harm, or other financial detriment suffered individually by Plaintiffs and the other members of the Class are relatively small compared to the burden and expense that would be required to litigate their claims on an individual basis against Defendants, making it impracticable for Class members to individually seek redress for Defendants' wrongful conduct. Even if Class members could afford individual litigation, the court system could not. Individualized litigation would create a potential for inconsistent or contradictory judgments and increase the delay and expense to all parties and the court system. By contrast, the class action device presents far fewer management difficulties and provides the benefits of single adjudication, economies of scale, and comprehensive supervision by a single court.

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

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

a. Whether Plaintiffs and the other Class members' PII was accessed, compromised, or stolen in the Data Breach;

b. Whether (and when) Defendants knew about any security

vulnerabilities that led to the Data Breach before they were announced to the public;

c. Whether Defendants had a duty to promptly notify Plaintiffs and the other Class members that their PII was, or potentially could be, compromised and failed to do so;

d. Whether Defendants' representations that they would secure and protect the PII of Plaintiffs and the other Class members were facts that reasonable persons could be expected to rely upon when deciding whether to use Defendants' services;

e. Whether Defendants misrepresented the safety of their many systems and services, specifically the security thereof, and their ability to safely store Plaintiffs' and the other Class members' PII;

f. Whether Defendants concealed crucial information about their inadequate data security measures from Plaintiffs and the other Class members;

g. Whether Defendants knew or should have known that they did not employ reasonable measures to keep Plaintiffs' and the other Class members' PII secure and prevent the loss or misuse of that information;

h. Whether Defendants owed a duty to Plaintiffs and the other Class members to safeguard their PII and to implement adequate data security measures, and whether Defendants breached that duty;

i. Whether Defendants' representations were false with regard to storing and safeguarding Plaintiffs' and the other Class members' PII; and

j. Whether Defendants' representations were material with regard to storing and safeguarding Plaintiffs' and the other Class members' PII.

FIRST CAUSE OF ACTION

Negligence

(On Behalf of the Nationwide Class)

73. Plaintiffs hereby repeat, reallege, and incorporate by reference each and every allegation contained above as though the same were fully set forth herein.

74. Plaintiffs bring this cause of action individually and on behalf of the Nationwide Class.

75. Defendants owed a duty to Plaintiffs and the other Class members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting and protecting their PII in Defendants' possession from being compromised, lost, stolen, accessed, misused, and/or disclosed to unauthorized parties. More specifically, this duty included, *inter alia*, (a) designing, maintaining, and testing Defendants' security systems to ensure that the PII of Plaintiffs and the other Class members in Defendants' possession was adequately secured and protected, including using encryption technologies; (b) implementing processes that would detect a breach of their security systems in a timely manner; (c) timely acting upon warnings and alerts, including those generated by Defendants' own security systems, regarding intrusions to their networks; and (d) maintaining data security measures consistent with industry standards.

76. Defendants knew or should have known that the PII of Plaintiffs and the other Class members included personal and sensitive information that is valuable to identity thieves and other criminals. Defendants also knew or should have known of the serious harms that could happen if the PII of Plaintiffs and the other Class members was wrongfully exposed, that exposure was not fixed, and/or Plaintiffs and the other Class members were not told about the exposure in a timely manner.

77. By entrusting Defendants to safeguard their PII, Plaintiffs and the other Class members had a special relationship with Defendants. Plaintiffs and the other Class members applied for Defendants' services and agreed to provide their PII with the understanding that Defendants would take appropriate measures to protect it, and would inform Plaintiffs and the other Class members of any breaches or other

security concerns that might call for action by them. But Defendants did not. Defendants not only knew that their data security was inadequate, they also knew they did not have the tools to detect and document intrusions or exfiltration of PII. Defendants are morally culpable, given their knowledge of cyberattacks on the real estate industry, wholly inadequate safeguards, and refusal to notify Plaintiffs and the other Class members of breaches or security vulnerabilities.

78. Defendants owed a duty of care to Plaintiffs and the other Class members because they were foreseeable and probable victims of any inadequate security practices. Not only was it foreseeable that Plaintiffs and the other Class members would be harmed by the failure to protect their PII because hackers routinely attempt to steal such information and use it for nefarious purposes, Defendants knew that it was more likely than not Plaintiffs and the other Class members would be harmed. Defendants solicited, gathered, and stored PII provided by Plaintiffs and the other Class members in the regular course of business. Since Defendants knew that a breach of their systems would cause damages to Plaintiffs and the other Class members, Defendants had a duty to adequately protect such sensitive personal information.

79. Defendants' duty to use reasonable data security measures also arose under Section 5 of the Federal Trade Commission Act ("FTC Act"), 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect personal information by companies such First American. Various FTC publications and data security breach orders further form the basis of First American's duty. In addition, individual states have enacted statutes based upon the FTC Act that also created a duty.

80. Defendants also had a duty to safeguard the PII of Plaintiffs and the other Class members and to promptly notify them of a breach based on state laws and statutes that require Defendants to reasonably safeguard PII, as detailed herein.

81. Defendants breached their duty to exercise reasonable care in safeguarding and protecting Plaintiffs' and the other Class members' PII by failing to adopt, implement, and maintain adequate security measures to safeguard that information, despite repeated failures and intrusions, and allowing unauthorized access to their PII.

82. Defendants' failure to comply with industry and federal regulations further evidences their negligence in failing to exercise reasonable care in safeguarding and protecting Plaintiffs' and the other Class members' PII.

83. Defendants' breaches of these duties were not merely isolated incidents or small mishaps. Rather, the breaches of the duties set forth above resulted from a long-term company-wide refusal by Defendants to acknowledge and correct serious and ongoing data security problems.

84. Defendants also owed a duty to Plaintiffs and the other Class members to timely disclose any incidents of data breaches, where such breaches compromised the PII of Plaintiffs and the other Class members. Timely notification was required, appropriate, and necessary so that, among other things, Plaintiffs and the other Class members could take appropriate measures to freeze or lock their credit profiles, avoid unauthorized charges to their credit or debit card accounts, cancel or change usernames and passwords on compromised accounts, monitor their account information and credit reports for fraudulent activity, contact their banks or other financial institutions that issue their credit or debit cards, obtain credit monitoring services, and take other steps to mitigate or ameliorate the damages caused by Defendants' misconduct. Plaintiffs and the other Class members were foreseeable and probable victims of any inadequate notice practices. Defendants knew that, through their actions and omissions, they had caused the sensitive PII of Plaintiffs and the other Class members to be compromised and accessed by unauthorized persons yet failed to mitigate potential harm to their customers by providing timely notice of the Data Breach.

85. But for Defendants' wrongful and negligent breach of their duties owed to Plaintiffs and the other Class members, their PII would not have been compromised, stolen, accessed and/or viewed by unauthorized persons.

86. As a direct, proximate and legal result of Defendants' negligence, Plaintiffs and the other Class members have been injured as described herein, and are entitled to damages in an amount to be proven at trial. Plaintiffs and the other Class members' injuries include, but are not limited to, the following:

a. purchasing goods and services they would not have otherwise paid for and/or paying more for good and services than they otherwise would have paid, had they known the truth about Defendants' substandard data security practices;
b. losing the inherent value of their PII;
c. losing the value of the explicit and implicit promises of data security;
d. identity theft and fraud resulting from the theft of their PII;
e. costs associated with the detection and prevention of identity theft and unauthorized use of their financial accounts;
f. costs associated with purchasing credit monitoring, credit freezes, and identity theft protection services;
g. unauthorized charges and loss of use of and access to their financial account funds and costs associated with inability to obtain money from their accounts or being limited in the amount of money they were permitted to obtain from their accounts, including missed payments on bills and loans, late charges and fees, and adverse effects on their credit;
h. lowered credit scores resulting from credit inquiries following fraudulent activities;
i. costs associated with time spent and the loss of productivity or the enjoyment of one's life from taking time to address and attempt to

mitigate and address the actual and future consequences of the Data Breach, including discovering fraudulent charges, cancelling and reissuing cards, purchasing credit monitoring and identity theft protection services, imposing withdrawal and purchase limits on compromised accounts, and the stress, nuisance and annoyance of dealing with the repercussions of the Data Breach; and

j. the continued imminent and certainly impending injury flowing from potential fraud and identify theft posed by their Personal Information being in the possession of one or many unauthorized third parties.

87. The injury and harm suffered by Plaintiffs and the other Class members was the reasonably foreseeable result of Defendants' failure to exercise reasonable care in safeguarding and protecting Plaintiffs' and the other Class members' PII. Defendants knew their systems and technologies for processing and securing the PII of Plaintiffs and the other Class members had numerous security vulnerabilities.

88. As a result of this misconduct by Defendants, the PII of Plaintiffs and the other Class members was compromised, placing them at a greater risk of identity theft or subjecting them to identity theft, and their PII was disclosed to third parties without their consent. Plaintiffs and the other Class members also suffered diminution in value of their PII in that it is now easily available to hackers on the dark web. In addition, Plaintiffs and the other Class members have also suffered consequential out-of-pocket losses for procuring credit freeze or protection services, identity theft monitoring, and other expenses relating to identity theft losses or protective measures.

89. Defendants' misconduct as alleged herein constitutes malice or oppression in that it was despicable conduct carried on by Defendants with a willful and conscious disregard of the rights or safety of Plaintiffs and the other Class members and that despicable conduct has subjected Plaintiffs and the other Class members to cruel and unjust hardship in conscious disregard of their rights. As a

result, Plaintiffs and the other Class members are entitled to injunctive relief, as well as, actual and punitive damages against Defendants.

SECOND CAUSE OF ACTION

Breach of Contract

(On Behalf of the Nationwide Class)

90. Plaintiffs hereby repeat, reallege, and incorporate by reference each and every allegation contained above as though the same were fully set forth herein.

91. Plaintiffs bring this cause of action individually and on behalf of the Nationwide Class.

92. Plaintiffs and the other Class members entered into a contract with First American for the provision of title insurance, a home warranty, or other closing services.

93. The terms of First American's Privacy Policy are part of the contract.

94. First American's Privacy Policy is an agreement between First American and individuals who provided their PII to First American, including Plaintiffs and other Class members, even after they are no longer a customer of First American.

95. First American's Privacy Policy "governs [First American's] use of the information [customers] provide us," and applies when First American receives information (1) from individuals "on applications, forms and in other communications to [First American], whether in writing, in person, by telephone or any other means"; (2) about individuals' "transactions with [First American, its] affiliated companies, or others"; and (3) about individuals "from a consumer reporting agency."[36]

96. Plaintiffs and the other Class members provided their PII to Defendants

[36] First American Privacy Information, *available at* http://web.archive.org/web/20190525235150/https:/www.firstam.com/privacy-policy/index.html (last visited April 20, 2020).

when they, among other things, applied for and/or purchased title insurance, a home warranty, and/or other real estate transaction closing services provided by Defendants.

97. Plaintiffs and the other Class members performed substantially all that was required of them under their contract with First American, or they were excused from doing so.

98. Conversely, First American, in collecting Plaintiffs' and the other Class members' PII, manifested its intent to adhere to its obligations under the Privacy Policy, including using its "best efforts to ensure that no unauthorized parties have access to any of [its customers'] information."[37]

99. Further, First American stated that it "currently maintain[s] physical, electronic, and procedural safeguards that comply with federal regulations to guard [customers'] nonpublic personal information.[38]

100. First American failed to perform its obligations under the contract, including failing to provide adequate privacy, security, and confidentiality safeguards for Plaintiffs' and the other Class members' information and documents.

101. As a direct and proximate result of First American's breach of contract, Plaintiffs and the other Class members did not receive the full benefit of the bargain, and instead received title insurance, a home warranty, and/or other closing services that were less valuable than described in their contracts. Plaintiffs and the other 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.

102. As an additional direct and proximate result of Defendants' breach of contract, Plaintiffs and the other Class members have suffered actual damages resulting from the exposure of their PII information, and they remain at imminent

[37] *Id.*

[38] *Id.*

risk of suffering additional damages in the future.

103. Accordingly, because Plaintiffs and the other Class members have been injured by Defendants' breach of contract, they are entitled to damages and/or restitution in an amount to be proven at trial.

THIRD CAUSE OF ACTION

Breach of Implied Contract

(On Behalf of the Nationwide Class)

104. Plaintiffs hereby repeat, reallege, and incorporate by reference each and every allegation contained above as though the same were fully set forth herein.

105. Plaintiffs bring this cause of action individually and on behalf of the Nationwide Class.

106. Defendants solicited and invited Plaintiffs and the other Class members to apply for their services. Plaintiffs and the other Class members accepted Defendants' offer and provided documents containing PII to Defendants, and if approved, money, in exchange for Defendants' title insurance, home warranty and/or other real estate transaction closing services.

107. When Plaintiffs and the other Class members applied for First American's services and products, they provided their PII. In so doing, Plaintiffs and the other Class members entered into implied contracts with First American pursuant to which it agreed to safeguard and protect their PII and to timely and accurately notify them if their PII was breached or compromised.

108. Each application for First American's service or product made by Plaintiffs and the other Class members was made pursuant to the mutually agreed-upon implied contract with First American under which it agreed to safeguard and protect their PII.

109. Plaintiffs and the other Class members entered into the implied contracts with the reasonable expectation that First American's data security practices and policies were reasonable and consistent with industry standards.

Plaintiffs and the other Class members believed that First American would use part of the monies paid to First American under the implied contracts to fund adequate and reasonable data security practices.

110. Plaintiffs and the other Class members would not have provided and entrusted their PII to First American or would have paid less for First American's services in the absence of the implied contract or implied terms between them and First American. The safeguarding of the PII of Plaintiffs and the other Class members and prompt and sufficient notification of a breach was critical to realize the intent of the parties.

111. Plaintiffs and the other Class members fully performed their obligations under the implied contracts with First American.

112. First American breached its implied contracts with Plaintiffs and the other Class members to safeguard and protect their PII when it (a) failed to have security protocols and measures in place to protect that information; (b) disclosed that information to unauthorized third parties; and (c) failed to provide timely and accurate notice that their PII was compromised as a result of the Data Breach.

113. As a direct and proximate result of First American's breaches of the implied contracts between it and Plaintiffs and the other Class members, Plaintiffs and the other Class members sustained actual losses and damages as described in detail above, including that they did not get the benefit of the bargain for which they paid.

FOURTH CAUSE OF ACTION

Breach of Confidence

(On Behalf of the Nationwide Class)

114. Plaintiffs hereby repeat, reallege, and incorporate by reference each and every allegation contained above as though the same were fully set forth herein.

115. Plaintiffs bring this cause of action individually, and on behalf of the Nationwide Class.

116. This claim is asserted against Defendants for breach of confidence concerning the PII that Plaintiffs and the other Class members provided to Defendants in confidence.

117. At all times during Plaintiffs' and the other Class members' interactions with Defendants, Defendants were fully aware of the confidential nature of the PII that Plaintiffs and the other Class members shared with Defendants.

118. Plaintiffs and the other Class members reasonably expected that their PII would be collected, stored, and protected in confidence by Defendants, and not disclosed to unauthorized third parties. Plaintiffs and the other Class members provided their respective PII to Defendants with the understanding that Defendants would protect and not permit that PII to be disseminated to any unauthorized third parties.

119. Defendants voluntarily received in confidence Plaintiffs' and the other Class members' PII with the understanding that that PII would not be disclosed or disseminated to the public or any unauthorized third parties.

120. On information and belief, due to Defendants' failure to prevent, detect, and stop the Data Breach from occurring, Plaintiffs' and the other Class members' PII was disclosed and misappropriated to unauthorized malicious third parties beyond their confidence and without their express permission.

121. Defendants' Privacy Policy contained an implied obligation on behalf of Defendants to promptly inform Plaintiffs and the other Class members of any breach by Defendants of their Privacy Policy and to take appropriate remedial measures to protect Plaintiffs' PII. This implied obligation is consistent with industry standards and practices related to large data breaches.

122. Following Defendants' failure to prevent, detect, and stop the Data Breach from occurring, Defendants failed to promptly inform Plaintiffs and the other Class members that their PII was disclosed, the extent of the breach, and any remedial measures Defendants have taken to remediate the breach or protect the

misappropriated PII.

123. As a direct and proximate cause of Defendants' actions and inactions, Plaintiffs and the other Class members have suffered injury and damages.

124. But for Defendants' exposure of PII in violation of the parties' understanding that it would be held in confidence, Plaintiffs' and the other Class members' PII would not have been compromised, stolen, and viewed by unauthorized persons. Defendants' exposure was a direct and legal cause of the theft of Plaintiffs' and the other Class members' PII, as well as their resulting damages.

125. The injury and harm Plaintiffs and the other Class members suffered was the reasonably foreseeable result of Defendants' unauthorized exposure of Plaintiffs' and the other Class members' PII. On information and belief, Defendants knew their computer systems and technologies for accepting and securing Plaintiffs' and the other Class members' PII had numerous security vulnerabilities, but Defendants continued to collect, store, and maintain Plaintiffs' and the other Class members' PII without fixing the vulnerabilities.

126. On information and belief, because of Defendants' misconduct, Plaintiffs' and the other Class members' PII was compromised – placing them at a greater risk of identity theft and subjecting them to identity theft and fraud – and disclosed to unauthorized, malicious, third parties without their consent. Plaintiffs and the other Class members also suffered diminution in value of their PII in that it became easily available to hackers on the dark web. Plaintiffs and the other Class members have also suffered consequential out-of-pocket losses for procuring credit freezes or protection services, identity theft monitoring, and other expenses relating to identity theft losses or protective measures.

FIFTH CAUSE OF ACTION

Violation of California Business and Professions Code § 17200, *et seq.*

(On Behalf of the Nationwide Class)

127. Plaintiffs hereby repeat, reallege, and incorporate by reference each

and every allegation contained above as though the same were fully set forth herein.

128. Plaintiffs bring this cause of action individually and on behalf of the Nationwide Class.

129. Defendants are "persons" as defined by California Businesss and Professions Code § 17201.

130. Defendants violated California Business and Professions Code § 17200, *et seq.* ("UCL") by engaging in unlawful, unfair, and deceptive business acts and practices.

131. California Business and Professions Code § 17200 prohibits acts of "unfair competition," including any "unlawful, unfair or fraudulent business act or practice" and "unfair, deceptive, untrue or misleading advertising."

132. Defendants' "unfair" acts and practices – all of which are immoral, unethical, oppressive, unscrupulous and/or substantially injurious to consumers – include:

a. Failing to implement and maintain reasonable security measures to protect Plaintiffs' and the other Class members' PII from unauthorized exposure, disclosure, release, data breaches, and theft, which was a direct and proximate cause of the Data Breach. Further, First American failed to identify foreseeable security risks, remediate identified security risks, and adequately improve security following the identification of security risks. This conduct, with little if any utility, is unfair when weighed against the harm to Plaintiffs and the other Class members, whose PII has been compromised.

b. Failing to implement and maintain reasonable security measures also was contrary to legislatively-declared public policy that seeks to protect consumers' data and ensure that entities that are trusted with it use appropriate security measures. These policies are reflected in laws, including the FTC Act, 15 U.S.C. § 45, and California's Consumer Records Act, Cal. Civ. Code § 1798.81.5.

c. Failing to implement and maintain reasonable security measures also lead to substantial consumer injuries, as described above, that are not outweighed by any countervailing benefits to consumers or competition. Moreover, because consumers could not know of Defendants' inadequate security, consumers could not have reasonably avoided the harms that Defendants caused.

d. Engaging in unlawful business practices by violating California Civil Code § 1798.82.

133. Defendants have engaged in "unlawful" business practices by violating multiple laws, including California's Consumer Records Act, Cal. Civ. Code §§ 1798.81.5 (requiring reasonable data security measures) and 1798.82 (requiring timely breach notification), California's Consumers Legal Remedies Act, Cal. Civ. Code §§ 1780, *et seq.*, the FTC Act, 15 U.S.C. § 45, and California common law.

134. Defendants' unlawful, unfair, and deceptive acts and practices include:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiffs and the other Class members' PII, which was a direct and proximate cause of the Data Breach;

b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following identified risks, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Class members' PII, including duties imposed by the FTC Act, 15 U.S.C. §45, and California's Customer Records Act, Cal. Civ. Code §§ 1798.80, *et seq.*, which was a direct and proximate cause of the Data Breach;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiffs and Class members' PII, including by

implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and California Subclass members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, and California's Customer Records Act, Cal. Civ. Code §§ 1798.80, *et seq.*;

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiffs and the other Class members' PII;

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and the other Class members' PI, including duties imposed by the FTC Act, 15 U.S.C. § 45, and California's Customer Records Act, Cal. Civ. Code § 1798.80, *et seq.*

135. Plaintiffs and the other Class members are reasonable consumers who expected Defendants to protect vigorously their Personal Information entrusted to Defendants and to be informed by Defendants of potential and actual cybersecurity vulnerabilities as soon as Defendants became aware of such threats.

136. Defendants' representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Defendants' data security and ability to protect the confidentiality of consumers' personal information.

137. Defendants' acts and omissions were intended to induce Plaintiffs and the other Class members' reliance on Defendants' promise that their PII was secure and protected and/or their failure to disclose otherwise, to increase the number of Class Members, and, ultimately, to increase Defendants' revenues. Plaintiffs and the other Class Members were deceived by Defendants' failure to properly implement adequate, commercially reasonable security measures to protect their

PII, and Defendants' failure to promptly notify them of the security breach. As a result, Defendants' conduct constitutes "fraudulent" business acts or practices.

138. Defendants' conduct was and is likely to deceive consumers.

139. In failing to implement adequate security procedures and protocols to protect Plaintiffs' and the other Class members' PII, and to promptly notify Plaintiffs and the other Class members of potential and actual security threats, Defendants have knowingly and intentionally concealed material facts and breached their duty not to do so.

140. Defendants were under a duty to Plaintiffs and the other Class members to protect Class Members' PII and promptly notify Class Members of potential and actual security threats, and other omitted facts alleged herein, because:

- Defendants were in a superior position to know the specifics of a potential or actual security breach; and
- Defendants actively concealed information known to them regarding potential and actual security breaches affecting Class Members' account information.
- Defendants have still not provided Plaintiffs and the other Class members with a comprehensive or detailed report on which customers were affected, and what information was stolen. Accordingly, Plaintiffs and the other victims of the Data Breach do not have the information they need to take informed and appropriate actions to mitigate the damage caused by the Data Breach and to protect against future acts of cyber-fraud.

141. The facts Defendants concealed from or did not disclose to Plaintiffs and the other Class members are material in that a reasonable person would have considered them to be important in deciding whether to use Defendants' services. Had Plaintiffs and other Class Members known that Defendants failed to employ necessary and adequate protection of their PII and would fail to timely notify them

of potential security breaches, they would not have used Defendants' services or would have paid much less for their services.

142. By their conduct, Defendants have engaged in unfair competition and unlawful, unfair and fraudulent business practices. Defendants' unfair or deceptive acts or practices occurred repeatedly in Defendants' trade or business and were capable of deceiving a substantial portion of the purchasing public.

143. As a direct and proximate result of Defendants' unlawful, unfair and deceptive acts and practices, Plaintiffs and the other Class members suffered and will continue to suffer injury in fact. Plaintiffs and the other Class members lost money or property as a result of purchasing services from Defendants, the premiums and/or price received by Defendants for their services, the loss of the benefit of their bargain with Defendants as they would not have paid Defendants for services or would have paid less for such services but for Defendants' violations alleged herein; losses from fraud and identity theft; costs for credit monitoring and identity protection services; time and expenses related to monitoring their financial accounts for fraudulent activity; loss of value of their PII; and an increased, imminent risk of fraud and identity theft.

144. Defendants acted intentionally, knowingly, and maliciously to violate California's Unfair Competition Law, and recklessly disregarded Plaintiffs and the other Class members' rights. Past data breaches within the industry put it on notice that its security and privacy protections were inadequate.

145. Defendants have been unjustly enriched and should be required to make restitution to Plaintiffs and the other Class members pursuant to §§17203 and 17204 of the California Business and Professions Code. Pursuant to California Business and Professions Code § 17203, Plaintiffs and the Class members seek an order of this Court enjoining Defendants from continuing to engage in unlawful, unfair, and fraudulent business practices and any other act prohibited by law, including those set forth in this Complaint.

146. Plaintiffs and the other Class members seek all monetary and non-monetary relief allowed by law, including restitution of all profits stemming from Defendants' unfair, unlawful, and fraudulent business practices or use of their PII; declaratory relief; reasonable attorneys' fees and costs under California Code of Civil Procedure § 1021.5; injunctive relief enjoining Defendants from continuing to employ deficient data security pursuant to California Business and Professions Code § 17203; and other appropriate equitable relief.

SIXTH CAUSE OF ACTION

Violation of California Consumers Legal Remedies Act

Cal. Civ. Code §1750, *et seq.*

(On Behalf of the Nationwide Class)

147. Plaintiffs hereby repeat, reallege, and incorporate by reference each and every allegation contained above as though the same were fully set forth herein.

148. Plaintiffs bring this cause of action individually and on behalf of the Nationwide Class.

149. The Consumers Legal Remedies Act, Cal. Civ. Code § 1750, *et seq.* ("CLRA") is a comprehensive statutory scheme that is to be liberally construed to serve its underlying purpose: Protecting consumers against unfair and deceptive business practices in connection with the conduct of businesses providing goods, property or services to consumers primarily for personal, family, or household use.

150. Defendants are "persons" as defined by Civil Code §§ 1761(c) and 1770, and has provided "services" as defined by Civil Code §§ 1761(b) and 1770.

151. California Civil 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."

152. In addition, Civil Code § 1770(a)(7) prohibits one who is involved in a transaction from "[r]epresenting that goods or services are of a particular standard, quality, or grade . . . if they are of another."

153. Plaintiffs and the other Class members are "consumers," as defined by Civil Code §§ 1761(d) and 1770, and have engaged in "transactions" with Defendants, as defined by Civil Code §§ 1761(e) and 1770.

154. Defendants acts and practices were intended to and did result in the sales of products and services to Plaintiffs and the other Class members in violation of Civil Code § 1770, including, but not limited to, the following:

a. Representing that services have characteristics that they do not have;
b. Representing that services are of a particular standard, quality, or grade when they were not;
c. Advertising services with intent not to sell them as advertised; and
d. Representing that the subject of a transaction has been supplied in accordance with a previous representation when it has not.

155. Defendants' representations and omissions were material because they were likely to and did deceive reasonable consumers about the adequacy of Defendants' data security and ability to protect the confidentiality of consumers' PII.

156. Had Defendants disclosed to Plaintiffs and the other class members that their data systems were not secure and, thus, vulnerable to attack, Defendants would have been unable to continue in business and would have been forced to adopt reasonable data security measures and comply with the law. Instead, Defendants received, maintained, and compiled Plaintiffs' and the other Class members' PII as part of the services Defendants provided and for which Plaintiffs and the other Class members paid without being advised that Defendants' data security practices were insufficient to maintain the safety and confidentiality of their PII. Accordingly, Plaintiffs and the other Class members acted reasonably in relying on Defendants' misrepresentations and omissions, the truth of which they could not have discovered

157. By misrepresenting that they took appropriate measures to protect Plaintiffs and the other Class members' PII, Defendants violated Civil Code § 1770.

158. Defendants' acts and omissions were intended to induce Plaintiffs and the other Class members' reliance on Defendants' promise that their PII was secure and protected and/or Defendants' failure to disclose otherwise, to increase the number of Class Members, and, ultimately, to increase Defendants' revenues. Plaintiffs and the other Class Members were deceived by Defendants' failure to properly implement adequate, commercially reasonable security measures to protect their PII.

159. As a result of their reliance on Defendants' representations and omissions, Plaintiffs and the other Class members suffered an ascertainable loss due to Defendants' failure to provide adequate protection of their personal and confidential information. This loss was also the direct result of Defendants' failure to provide timely and sufficiently informative notice and warning of potential and actual cybersecurity breaches.

160. As a result of engaging in such unfair methods of competition and unfair or deceptive acts or practices, Defendants have violated Civil Code §1770.

161. As a direct and proximate result of Defendants' violations of Civil Code § 1770, Plaintiffs and the other Class members suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including loss of the benefit of their bargain with Defendants as they would not have paid Defendants for services or would have paid less for such services but for Defendants' violations alleged herein; losses from fraud and identity theft; costs for credit monitoring and identity protection services; time and expenses related to monitoring their financial accounts for fraudulent activity; time and money spent cancelling and replacing credit cards; loss of value of their PII; and/or an increased, imminent risk of fraud and identity theft. Plaintiffs and the other Class Members lost money or property as a result of applying for services from Defendants.

162. Plaintiffs and the other Class members have provided notice of their

claims for damages to Defendants, in compliance with California Civil Code § 1782(a).

163. Plaintiffs and the other Class members seek all monetary and non-monetary relief allowed by law, including damages, an order enjoining the acts and practices described above, attorneys' fees, and costs under the CLRA.

SEVENTH CAUSE OF ACTION

Deceit by Concealment, Cal. Civ. Code §§ 1709, 1710

(On Behalf of the Nationwide Class)

164. Plaintiffs hereby repeat, reallege, and incorporate by reference each and every allegation contained above as though the same were fully set forth herein.

165. Plaintiffs bring this cause of action individually and on behalf of the Nationwide Class.

166. At the time Plaintiffs and the other Class Members provided their PII to Defendants, Defendants had an obligation to disclose to Plaintiffs and the other Class members that their PII was an easy target for hackers and Defendants were not implementing measures to protect them.

167. Defendants failed to make the required disclosures when they requested and received Plaintiffs and the other Class members' PII. Instead, Defendants willfully deceived Plaintiffs and the other Class members by concealing the true facts concerning their data security, which Defendants were obligated and had a duty to disclose, and by willfully allowing their customers to rely upon Defendants' false assurances that their PII and other data was safe and that Defendants were dedicated to maintaining that security.

168. Had Defendants disclosed the true facts about their poor data security, Plaintiffs and the other Class members would have taken measures to protect themselves or used another company for their title insurance, home warranty, and/or other real estate transaction closing services. Plaintiffs and the other Class members justifiably relied on Defendants to provide accurate and complete information about

Defendants' data security, and Defendants did not. Further, independent of any representations made by Defendants, Plaintiffs and the other Class members justifiably relied on Defendants to provide title insurance, a home warranty, and/or other real estate transaction closing services with at least minimally adequate security measures and justifiably relied on Defendants to disclose facts undermining that reliance.

169. Rather than cease offering a clearly unsafe and defective services or disclosing to Plaintiffs and the other Class members that their services were unsafe and users' PII was exposed to theft on a grand scale, Defendants continued and concealed information relating to the inadequacy of their security.

170. These actions are "deceit" under Civil Code § 1710 in that they are the suppression of a fact, by one who is bound to disclose it, or who gives information of other facts which are likely to mislead for want of communication of that fact.

171. As a result of this deceit by Defendants, they are liable under Civil Code § 1709 for "any damage which [Plaintiffs and the Class] thereby suffer[]."

172. Because of this deceit by Defendants, the PII of Plaintiffs and the other Class members was compromised, placing them at a greater risk of identity theft and subjecting them to identity theft, and their PII was disclosed to third parties without their consent. Plaintiffs and the other Class members also suffered diminution in value of their PII in that it is now easily available to hackers on the Dark Web. Plaintiffs and/or the other Class members have also suffered consequential out of pocket losses for procuring credit freeze or protection services, identity theft monitoring, and/or other expenses relating to identity theft losses or protective measures.

173. Defendants' deceit as alleged herein is fraud under California Civil Code § 3294(c)(3) in that it was deceit or concealment of a material fact known to the Defendants conducted with the intent on the part of Defendants of depriving Plaintiffs and the other Class members of "legal rights or otherwise causing injury."

As a result, Plaintiffs and the other Class members are entitled to punitive damages against Defendants under California Civil Code § 3294(a).

EIGHTH CAUSE OF ACTION

Violation of the California Customer Records Act

Cal. Civ. Code § 1798.80, *et seq*.

(On Behalf of the California Sub-Class)

174. Plaintiffs Dinh, Forney, Campbell, and Schaadt ("CA Plaintiffs") hereby repeat, reallege, and incorporate by reference each and every allegation contained above as though the same were fully set forth herein.

175. CA Plaintiffs bring this cause of action individually and on behalf of themselves and the California Sub-Class.

176. "[T]o ensure that personal information about California residents is protected," the California Legislature enacted California Civil Code ("Civil Code") § 1798.81.5, which requires that any business that "owns, licenses, or maintains personal information about a California resident … 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."

177. Defendants are "businesses," as defined by Civil Code § 1798.80(a), that own, maintain and license PII within the meaning of § 1798.81.5, about CA Plaintiffs and California Sub-class members.

178. Businesses that own or license computerized data that includes PII are required to notify California residents when their Personal Information has been acquired (or is reasonably believed to have been acquired) by unauthorized persons in a data security breach "in the most expedient time possible and without unreasonable delay." Cal. Civ. Code § 1798.82. Among other requirements, the security breach notification must include "the types of Personal Information that were or are reasonably believed to have been the subject of the breach." Cal. Civ.

Code § 1798.82.

179. Defendants are businesses that own or license computerized data that includes PII as defined by Civil Code § 1798.82.

180. CA Plaintiffs and the other California Sub-Class members are "individual[s]" as defined by Civil Code § 1798.80(d).

181. CA Plaintiffs and the other California Sub-Class members' PII compromised, accessed and/or taken in the Data Breach includes "personal information" as defined by Civil Code §§ 1798.80(e), 1798.81.5(d) and 1798.82, which includes:

> "information that identifies, relates to, describes, or is capable of being associated with, a particular individual, including, but not limited to, his or her name, signature, Social Security number, physical characteristics or description, address, telephone number, passport number, driver's license or state identification card number, insurance policy number, education, employment, employment history, bank account number, credit card number, debit card number, or any other financial information, medical information, or health insurance information."

182. The breach of CA Plaintiffs and the other California Sub-Class members' PII was a "breach of the security system" of Defendant as defined by Civil Code § 1798.82(g).

183. By failing to implement reasonable security measures which would appropriately secure CA Plaintiffs and the other California Sub-Class members' PII, Defendants violated Civil Code § 1798.81.5.

184. In addition, by failing to notify in a timely and accurate fashion all affected California Sub-Class members that their PII had been or may have been acquired by unauthorized persons in the Data Breach, Defendants violated Civil Code § 1798.82.

185. As a direct and proximate result of Defendants' violations of Civil

Code §§ 1798.81.5 and 1798.82, CA Plaintiffs and the California Sub-Class members suffered damages because they have lost the opportunity to immediately:

a. buy identity protection, monitoring, and recovery services;

b. flag asset, credit, and tax accounts for fraud, including reporting the theft of their Social Security numbers to financial institutions, credit agencies, and the Internal Revenue Service;

c. purchase or otherwise obtain credit reports, monitor credit, financial, utility, explanation of benefits, and other account statements on a monthly basis for unrecognized credit inquiries, Social Security numbers, home addresses, charges, and/or medical services;

d. place and renew credit fraud alerts on a quarterly basis;

e. routinely monitor public records, loan data, or criminal records;

f. contest fraudulent charges and other forms of criminal, financial and medical identity theft, and repair damage to credit and other financial accounts; and

g. take other steps to protect themselves and recover from identity theft and fraud.

186. In addition, because of Defendants' violation of Civil Code § 1798.81.5, CA Plaintiffs and the other California Sub-Class members have incurred and will incur damages including, but not necessarily limited to:

a. the loss of the opportunity to control how their PII is used;

b. the diminution in the value and/or use of their PII entrusted to Defendants for the purpose of deriving services from Defendants and with the understanding that Defendants would safeguard their PII against theft and not allow access and misuse of their PII by others;

c. the compromise, publication, and/or theft of their PII, out-of-pocket costs associated with the prevention, detection, and recovery from identity theft and/or unauthorized use of financial and medical

accounts;

d. lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the breach including, but not limited to, efforts spent researching how to prevent, detect, contest and recover from identity data misuse;

e. costs associated with the ability to use credit and assets frozen or flagged due to credit misuse, including complete credit denial and/or increased costs to use credit, credit scores, credit reports and assets;

f. unauthorized use of compromised PII to open new financial and/or health care or medical accounts, tax fraud and/or other unauthorized charges to financial, health care or medical accounts and associated lack of access to funds while proper information is confirmed and corrected;

g. the continued risk to their PII, which remain in Defendants' possession and are subject to further breaches so long as Defendants fail to undertake appropriate and adequate measures to protect the PII in their possession; and

h. future costs in terms of time, effort and money that will be expended, to prevent, detect, contest, and repair the impact of the PII compromised as a result of the Data Breach for the remainder of the lives of the California Sub-Class members.

187. Because they violated Civil Code §§ 1798.81.5 and 1798.82, Defendants "may be enjoined" under Civil Code § 1798.84(e).

188. CA Plaintiffs request that the Court enter an injunction requiring Defendants to inform Class members of the Data Breach and implement and maintain reasonable security procedures to protect CA Plaintiffs and the other California Sub-Class members' PII including, but not limited to, ordering that

Defendants:

a. engage third party security auditors/penetration testers as well as internal security personnel to conduct testing consistent with prudent industry practices, including simulated attacks, penetration tests, and audits on Defendants' systems on a periodic basis;

b. engage third party security auditors and internal personnel to run automated security monitoring consistent with prudent industry practices;

c. audit, test, and train their security personnel regarding any new or modified procedures;

d. conduct regular database scanning and securing checks consistent with prudent industry practices;

e. periodically conduct internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach consistent with prudent industry practices;

f. receive periodic compliance audits by a third party regarding the security of the computer systems, cloud-based services, and application software Defendants use to store the PII of California Sub-Class Members;

g. meaningfully educate California Sub-Class Members about the threats they face because of the loss of their PII to third parties, as well as the steps they must take to protect themselves; and

h. provide ongoing identity theft protection, monitoring, and recovery services to Plaintiffs and the other California Sub-Class members.

189. CA Plaintiffs seek all remedies available under Civil Code § 1798.84, including actual and statutory damages, equitable relief, and reasonable attorneys' fees. CA Plaintiffs also seek reasonable attorneys' fees and costs under applicable

law including California Code of Civil Procedure § 1021.5.

NINTH CAUSE OF ACTION

New York General Business Law, N.Y. Gen. Bus. Law § 349, *et seq.*

(On Behalf of the New York Sub-Class)

190. Plaintiff Abdelrasoul ("NY Plaintiff") hereby repeats, realleges, and incorporate by reference paragraphs 1-171 as though the same were fully set forth herein.

191. NY Plaintiff bring this cause of action individually and on behalf of himself and the New York Sub-Class.

192. Defendants engaged in deceptive acts or practices in the conduct of their business, trade, and commerce or furnishing of services, in violation of N.Y. Gen. Bus. Law § 349, including:

a. Failing to implement and maintain reasonable security and privacy measures to protect NY Plaintiff and New York Sub-Class members' PII, which was a direct and proximate cause of the Data Breach;

b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of NY Plaintiff and New York Sub-Class members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, which was a direct and proximate cause of the Data Breach;

d. Misrepresenting that they would protect the privacy and confidentiality of NY Plaintiff and New York Sub-Class members' PII, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that they would comply with common law and statutory duties pertaining to the security and privacy of NY Plaintiff

and New York Sub-Class members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45;

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure NY Plaintiff and New York Sub-Class members' PII; and

g. Omitting, suppressing, and concealing the material fact that they did not comply with common law and statutory duties pertaining to the security and privacy of NY Plaintiff and New York Sub-Class members' PII, including duties imposed by the FTC Act, 15 F.T.C. § 45.

193. NY Plaintiff and members of the New York Sub-Class were deceived in New York. They also transacted with Defendants in New York by purchasing title insurance, home warranties, and/or other real estate transaction closing services in New York.

194. Defendants' representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Defendants' data security and ability to protect the confidentiality of consumers' PII.

195. Defendants acted intentionally, knowingly, and maliciously to violate New York's General Business Law, and recklessly disregarded NY Plaintiff and New York Sub-Class members' rights. Past data breaches within the industry put Defendants on notice that their security and privacy protections were inadequate.

196. As a direct and proximate result of Defendants' deceptive and unlawful acts and practices, NY Plaintiff and New York Sub-Class members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including loss of the benefit of their bargain with Defendants as they would not have paid Defendants for services or would have paid less for such services but for Defendants' violations alleged herein; losses from fraud and identity theft; costs for credit monitoring and identity protection services;

time and expenses related to monitoring their financial accounts for fraudulent activity; loss of value of their PII; and an increased, imminent risk of fraud and identity theft.

197. Defendants' deceptive and unlawful acts and practices complained of herein affected the public interest and consumers at large, including the New Yorkers affected by the Data Breach.

198. The above deceptive and unlawful practices and acts by Defendants caused substantial injury to NY Plaintiff and New York Sub-Class members that they could not reasonably avoid.

199. NY Plaintiff and New York Sub-Class members seek all monetary and non-monetary relief allowed by law, including actual damages or statutory damages of $50 (whichever is greater), treble damages, restitution, injunctive relief, and attorney's fees and costs.

PRAYER FOR RELIEF

200. Plaintiffs, on behalf of themselves and all others similarly situated, request the Court to enter judgment against Defendants, as follows:

a. Certifying the Nationwide Class and appointing Plaintiffs as the Class Representatives for the Nationwide Class, or in the alternative, certifying the California Sub-Class and the New York Sub-Class and appointing Plaintiffs Dinh, Forney, Campbell, and Schaadt as Class Representatives for the California Sub-Class, and Plaintiff Abdelrasoul as Class Representative for the New York Sub-Class;

b. Appointing Jordan S. Esensten of Esensten Law and Ivy T. Ngo of Garner & Associates, LLP as Class Counsel for the Nationwide Class, or in the alternative, the California Sub-Class and New York Sub-Class;

c. Finding that Defendants' conduct was negligent, in breach of contract and implied contract, and unlawful as alleged herein;

d. An order permanently enjoining Defendants from further unfair, unlawful, and deceptive business acts and practices described herein;

e. Awarding Plaintiffs and the other Class, or in the alternative, Sub-Class members actual, compensatory, and consequential damages;

f. Awarding Plaintiffs and the other Class, or in the alternative, Sub-Class members restitution and disgorgement;

g. Requiring Defendants to provide appropriate credit monitoring services to Plaintiffs and the other Class, or in the alternative, Sub-Class members;

h. Awarding Plaintiffs and the other Class, or in the alternative, Sub-Class members punitive damages;

i. Awarding Plaintiffs and the other Class, or in the alternative, Sub-Class members pre-judgment and post-judgment interest;

j. Awarding Plaintiffs and the other Class, or in the alternative, Sub-Class members reasonable attorneys' fees, costs and expenses; and

k. Granting such other relief as the Court deems just and proper.

DEMAND FOR JURY TRIAL

201. Pursuant to Federal Rule of Civil Procedure 38(b) and Central District of California Local Rule 38-1, Plaintiffs demand a trial by jury of all issues in this action so triable.

Dated: April 20, 2020

Respectfully submitted,

By: */s/ Ivy T. Ngo*

Ivy T. Ngo (SBN 249860)
ivy@garner-associates.com
GARNER & ASSOCIATES LLP
520 Capitol Mall, Suite 289
Sacramento, CA 95814
Telephone: (530) 934-3324
Facsimile: (530) 934-2334

Jordan S. Esensten (SBN 264645)

jesensten@esenstenlaw.com
ESENSTEN LAW
12100 Wilshire Blvd., Suite 1660
Los Angeles, CA 90025
Telephone: (310) 273-3090
Facsimile: (310) 207-5969

Interim Co-Lead Counsel for Plaintiffs and Putative Class

The filer hereby attests that the filer has the consent and authority of all signatories and counsel listed herein

CERTIFICATE OF SERVICE

I hereby certify that on April 20, 2020, I electronically transmitted the attached document to the Clerk's Office using the CM/ECF System for filing and transmittal of a Notice of Electronic Filing to the CM/ECF registrants for this case.

*/s/ Ivy T. Ngo*_____
Ivy T. Ngo