

1 Tina Wolfson, SBN 174806
2 twolfson@ahdootwolfson.com
3 Theodore Maya, SBN 223242
4 tmaya@ahdootwolfson.com
5 Alex R. Straus, SBN 321366
6 astraus@ahdootwolfson.com
7 AHDOOT & WOLFSON, PC
8 10728 Lindbrook Drive
9 Los Angeles, CA 90024
10 Tel: 310-474-9111
11 Fax: 310-474-8585

12 *Attorneys for Plaintiff Fred Shakib*

13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

**UNITED STATES DISTRICT COURT
CENTRAL DISTRICT OF CALIFORNIA**

FRED SHAKIB, individually and on
behalf of all others similarly situated,

Plaintiff,

v.

FIRST AMERICAN FINANCIAL
CORPORATION,

Defendant.

Case No. 8:19-cv-1022

CLASS ACTION COMPLAINT

Plaintiff Fred Shakib (“Mr. Shakib” or “Plaintiff”), individually and on behalf of the proposed Classes defined below, allege as follows upon personal knowledge as to themselves and their own experiences and, as to all other matters, upon information and belief including investigation conducted by their attorneys.

NATURE OF THE CASE

1
2 1. Plaintiff brings this class action lawsuit against First American Financial
3 Corporation (“FAFC” or “Defendant”) because of its failure to protect the confidential
4 information of millions of consumers—including their names, bank account numbers,
5 bank account statements, mortgage records, tax records, Social Security numbers, wire
6 transaction receipts, drivers’ license images, and other personal financial information
7 (collectively, their “Personal Information”).

8 2. FAFC is one of the largest title insurance companies in the United States
9 with more than 18,000 employees and \$5.7 billion in revenue in 2018.

10 3. FAFC provides title insurance, closing/settlement services, property data,
11 automated title plant records, home warranty products, property and casualty insurance,
12 trust and wealth management services, and other related products and services.

13 4. In order to utilize the services provided by FAFC, an individual must
14 provide his or her Personal Information. FAFC stores this information indefinitely,
15 including the period after which any customer relationship has ceased.¹

16 5. FAFC expressly promises it will maintain appropriate facilities and systems
17 to protect against unauthorized access to and corruption of its customers’ Personal
18 Information.²

19 6. FAFC expressly promises it will use its best efforts to ensure that no
20 unauthorized parties have access to any of its customers’ Personal Information.³

21 7. FAFC expressly promises it will restrict access to nonpublic Personal
22 Information about its customers to those individuals and entities who need to know that
23 information to provide products or services.⁴

24
25
26 ¹ <https://www.firstam.com/privacy-policy/> (last viewed May 26, 2019)

27 ² *Id.*

28 ³ *Id.*

⁴ *Id.*

1 8. FAFC expressly promises it maintains physical, electronic, and procedural
2 safeguards that comply with federal regulations to guard its customers' nonpublic
3 Personal Information.⁵

4 9. On May 24, 2019, it was revealed that FAFC's failure to protect its
5 customers' Personal Information resulted in the exposure of approximately 885 million
6 records related to mortgage deals dating back 16 years. Many of the exposed files are
7 records of wire transactions with bank account numbers and other Personal Information
8 from both home/property buyers and sellers.

9 10. In one of the most reckless data breaches/exposures in modern history, the
10 FAFC website allowed anyone with a computer to access approximately 885 million
11 records without asking for any authentication. The only action required to exploit the
12 vulnerability in FAFC's website was tweaking a single digit in the address of a file. No
13 password or other login credentials were required to access all of FAFC's customers'
14 files and Personal Information.

15 11. FAFC not only failed to provide the level of data protection that it expressly
16 promised, it also exposed millions of individuals' Personal Information to an increased
17 risk of misuse by unauthorized third parties (*e.g.*, identity theft).

18 12. Had FAFC informed its customers that it would use inadequate security
19 measures, consumers (like Plaintiff and the members of the Classes) would not have been
20 willing to sign up for or pay for its title insurance and other services at the price charged,
21 if at all.

22 13. FAFC's failure to implement adequate security protocols jeopardized
23 millions of consumers' Personal Information, fell well short of its promises, and
24 diminished the value of the services provided. In other words, because FAFC failed to
25 disclose its gross security inadequacies, it delivered a fundamentally less useful and less
26 valuable service than the one paid for.

27
28 _____
⁵ *Id.*

1 14. Accordingly, Plaintiff brings suit on behalf of themselves and all others
2 similarly situated, to seek redress for FAFC's unlawful conduct.

3
4 **PARTIES**

5 15. Plaintiff Fred Shakib is a resident and citizen of the State of California.

6 16. Defendant First American Financial Corporation is a Delaware Corporation
7 with its headquarters and principal place of business located in Santa Ana, California.

8
9 **JURISDICTION AND VENUE**

10 17. This Court has subject matter jurisdiction over this action pursuant to 28
11 U.S.C. § 1332(d)(2) because (a) at least one member of the putative Classes is a citizen
12 of a state different from Defendant, and (b) the amount in controversy exceeds
13 \$5,000,000, exclusive of interest and costs.

14 18. This Court has personal jurisdiction over Defendant because it is registered
15 to and regularly does conduct business in this District, and the unlawful conduct alleged
16 in this Complaint occurred in, was directed to, and/or emanated, in part, from this District.

17 19. Venue is proper pursuant to 28 U.S.C. § 1391(b) because a substantial part
18 of the events or omissions giving rise to the unlawful conduct alleged in this Complaint
19 occurred in, was directed to, and/or emanated from this District. Venue is additionally
20 proper because Defendant is registered to and does conduct business in this District.

21
22 **FACTUAL BACKGROUND**

23 **I. FAFC Promised To Protect Its Customers' Personal Information From**
24 **Unauthorized Disclosures.**

25 20. FAFC promised it would keep its customers' Personal Information
26 confidential and protect it from unauthorized disclosure. For instance, the PRIVACY
27 INFORMATION appearing on FAFC's primary website states, in relevant part:⁶

28 _____
⁶ *Id.*

1
2 **We Are Committed to Safeguarding Customer Information**

3 In order to better serve your needs now and in the future, we may ask you to
4 provide us with certain information. We understand that you may be
5 concerned about what we will do with such information - particularly any
6 personal or financial information. We agree that you have a right to know how
7 we will utilize the personal information you provide to us. Therefore, together
8 with our subsidiaries we have adopted this Privacy Policy to govern the use
9 and handling of your personal information.

10 ...

11 We request information from you for our own legitimate business purposes
12 and not for the benefit of any nonaffiliated party. Therefore, we will not
13 release your information to nonaffiliated parties except: (1) as necessary for
14 us to provide the product or service you have requested of us; or (2) as
15 permitted by law. We may, however, store such information indefinitely,
16 including the period after which any customer relationship has ceased.

17 21. FAFC recognizes the importance of keeping consumers' Personal
18 Information private and repeatedly promises to protect that information and comply with
19 the data security requirements mandated by, among other things, federal regulations:

20 **Confidentiality and Security**

21 We will use our best efforts to ensure that no unauthorized parties have access
22 to any of your information. We restrict access to nonpublic personal
23 information about you to those individuals and entities who need to know that
24 information to provide products or services to you. We will use our best efforts
25 to train and oversee our employees and agents to ensure that your information
26 will be handled responsibly and in accordance with this Privacy Policy and
27 First American's Fair Information Values. We currently maintain physical,
28 electronic, and procedural safeguards that comply with federal regulations to
guard your nonpublic personal information.

...

Use We believe we should behave responsibly when we use information about
a consumer in our business. We will obey the laws governing the collection,
use and dissemination of data.

1
2 22. FAFC recognizes the particular significance of keeping consumers' Personal
3 Information obtained through its website and assured its customers transparency
4 regarding how such information would be treated:

5 **Information Obtained Through Our Web Site**

6 First American Financial Corporation is sensitive to privacy issues on the
7 Internet. We believe it is important you know how we treat the information
8 about you we receive on the Internet.

9 23. FAFC promised to be an industry leader in protecting the Personal
10 Information of its customers:

11 **Education** We endeavor to educate the users of our products and services, our
12 employees and others in our industry about the importance of consumer
13 privacy. We will instruct our employees on our fair information values and on
14 the responsible collection and use of data. We will encourage others in our
15 industry to collect and use information in a responsible manner.

16 **Security** We will maintain appropriate facilities and systems to protect
17 against unauthorized access to and corruption of the data we maintain.

18 24. On May 24, 2019, FAFC admitted that "a design defect in an application []
19 made possible unauthorized access to customer data."

20 25. In reality, FAFC exposed 885 million records to anyone with internet access
21 and a smartphone or computer.

22 26. The Personal Information of FAFC's customers was available for download
23 without hacking into the FAFC databases and without having to provide any
24 authentication. No password or other login credentials were required to access all of
25 FAFC's customers' files and Personal Information via the internet.

26 27. FAFC's security policies and practices were such that the only action
27 required to exploit the vulnerability in FAFC's website was tweaking a single digit in the
28 address of a file.

1 28. FAFC's security policies and practices were such that it never discovered
2 the vulnerability in its own system.

3 29. A real estate developer in Washington state discovered he could access the
4 Personal Information of all FAFC's customers people simply by modifying a single digit
5 in the internet link to any other FAFC document.

6 30. FAFC was reportedly nonresponsive when a it was first put on notice that
7 approximately 885 million records were potentially exposed.

8 31. Upon information and belief, the exposed Personal Information dates back
9 to 2003 and includes Personal Information from both sellers and buyers.

10
11 **II. FAFC Violated the Gramm-Leach-Bliley Act and Industry Standard Data**
12 **Protection Protocols.**

13 32. FAFC is a financial institution, as that term is defined by Section 509(3)(A)
14 of the Gramm-Leach-Bliley ("GLB") Act, 15 U.S.C. § 6809(3)(A), and is subject to the
15 GLB Act.

16 33. The GLB Act defines a financial institution as "any institution the business
17 of which is engaging in financial activities as described in Section 1843(k) of Title 12
18 (The Bank Holding Company Act of 1956')." 15 U.S.C. § 6809(3)(A).

19 34. Among other things, FAFC is significantly engaged in insuring,
20 guaranteeing, or indemnifying against loss, harm, damage, illness, disability, or death"
21 which is one of the activities listed as financial in nature under the Bank Holding
22 Company Act of 1956, 12 U.S.C. § 1843(k)(A).

23 35. FAFC collects nonpublic personal information, as defined by 16 C.F.R. §
24 313.3(n). Because FAFC is a financial institution that collects nonpublic personal
25 information, during the relevant time period it was subject to the requirements of the GLB
26 Privacy Rule, 16 C.F.R. § 313.1 et seq., and is subject to the requirements of Reg. P, 12
27 C.F.R. Part 1016, and the GLB Safeguards Rule, 16 C.F.R. § 314.1 et seq. Privacy Rule
28 and Reg. P 36.

1 36. The Privacy Rule, which implements Sections 501-503 of the GLB Act, 15
2 U.S.C. §§ 6801-6803, was promulgated by the Commission on May 24, 2000, and
3 became effective on July 1, 2001. See 16 C.F.R. Part 313. Since the enactment of the
4 Dodd-Frank Act on July 21, 2010, the CFPB became responsible for implementing the
5 Privacy Rule, and accordingly promulgated the Privacy of Consumer Financial
6 Information, Regulation P, 12 C.F.R. Part 1016 (“Reg. P”), which became effective on
7 October 28, 2014.

8 37. Accordingly, FAFC’s conduct is governed by the Privacy Rule prior to
9 October 28, 2014, and by Reg. P after that date.

10 38. Both Reg. P and the Privacy Rule require financial institutions to provide
11 customers with an initial and annual privacy notice. These privacy notices must be “clear
12 and conspicuous.” 16 C.F.R. §§ 313.4 and 313.5; 12 C.F.R. §§ 1016.4 and 1016.5. “Clear
13 and conspicuous means that a notice is reasonably understandable and designed to call
14 attention to the nature and significance of the information in the notice.” 16 C.F.R. §
15 313.3(b)(1); 12 C.F.R. § 1016.3(b)(1). These privacy notices must “accurately reflect[]
16 [the financial institution’s] privacy policies and practices.” 16 C.F.R. § 313.4 and 313.5;
17 12 C.F.R. §§ 1016.4 and 1016.5. They must include specified elements, including the
18 categories of nonpublic personal information the financial institution collects and
19 discloses, the categories of third parties to whom the financial institution discloses the
20 information, and the security and confidentiality policies of the financial institution. 16
21 C.F.R. § 313.6; 12 C.F.R. § 1016.6. These privacy notices must be provided “so that
22 each consumer can reasonably be expected to receive actual notice.” 16 C.F.R. § 313.9;
23 12 C.F.R. § 1016.9.

24 39. The Safeguards Rule, which implements Section 501(b) of the GLB Act, 15
25 U.S.C. § 6801(b), requires financial institutions to protect the security, confidentiality,
26 and integrity of customer information by developing a comprehensive written
27 information security program that contains reasonable administrative, technical, and
28 physical safeguards, including: (1) designating one or more employees to coordinate the

1 information security program; (2) identifying reasonably foreseeable internal and
2 external risks to the security, confidentiality, and integrity of customer information, and
3 assessing the sufficiency of any safeguards in place to control those risks; (3) designing
4 and implementing information safeguards to control the risks identified through risk
5 assessment, and regularly testing or otherwise monitoring the effectiveness of the
6 safeguards' key controls, systems, and procedures; (4) overseeing service providers and
7 requiring them by contract to protect the security and confidentiality of customer
8 information; and (5) evaluating and adjusting the information security program in light
9 of the results of testing and monitoring, changes to the business operation, and other
10 relevant circumstances. 16 C.F.R. §§ 314.3 and 314.4.

11 40. Until at least May 2019, FAFC failed to assess reasonably foreseeable
12 internal and external risks to the security, confidentiality, and integrity of customer
13 information.

14 41. Until approximately May 2019, FAFC failed to implement basic safeguards
15 to protect the security, confidentiality, and integrity of consumer information.

16 42. FAFC's conduct and lack thereof, resulted in a variety of failures to follow
17 GLB mandated data-security protocols, many of which are also industry standard. Among
18 such deficient practices, FAFC's breach shows that it failed to implement (or
19 inadequately implemented) information security policies or procedures such as effective
20 employee training, adequate intrusion detection systems, regular reviews of audit logs
21 and records, and other similar measures to protect the confidentiality of the Personal
22 Information it maintained in its data systems.

23 43. More specifically, FAFC's security failures demonstrate that it failed to
24 honor its express and implied promises by failing to:

- 25 a. Maintain an adequate data security system to reduce the risk of data breaches
26 and cyber attacks;
- 27 b. Adequately protect Plaintiff's and the Classes' Personal Information;

28

- c. Implement policies and procedures to prevent, detect, contain, and correct security violations;
- d. Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking report);
- e. Protect against any reasonably anticipated threats or hazards to the security or integrity of Personal Information;
- f. Effectively train all members of its workforce on the policies and procedures with respect to Personal Information as necessary and appropriate for the members of its workforce to carry out their functions and to maintain security of Personal Information.

44. Had FAFC implemented the above-described data security protocols, the consequences of the data exposure could have been avoided, or at least significantly reduced (as the exposure could have been detected earlier, the amount of Personal Information compromised could have been greatly reduced, and affected consumers could have been notified—and taken protective/mitigating actions—much sooner).

45. FAFC failed to fulfill its duties to those members who relied upon FAFC to competently manage, administer, and/or control their title insurance by not implementing the aforementioned security measures to adequately protect their Personal Information.

III. It is Well Established That Security Breaches Lead to Instances of Identity Theft.

46. The United States Government Accountability Office noted in a June 2007 report on Data Breaches (“GAO Report”) that identity thieves use identifying data such as SSNs to open financial accounts, receive government benefits and incur charges and credit in a person’s name.⁷ As the GAO Report states, this type of identity theft is the

⁷ See *Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown* (June 2007), United

1 most harmful because it may take some time for the victim to become aware of the theft
2 and can adversely impact the victim’s credit rating.

3 47. In addition, the GAO Report states that victims of identity theft will face
4 “substantial costs and inconveniences repairing damage to their credit records” and their
5 “good name.”⁸

6 48. According to the Federal Trade Commission (“FTC”), identity theft victims
7 must spend countless hours and large amounts of money repairing the impact to their
8 credit.⁹ Identity thieves use stolen personal information such as SSNs for a variety of
9 crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud.¹⁰

10 49. With access to an individual’s Personal Information, criminals can do more
11 than just empty a victim’s bank account—they can also commit various types of fraud,
12 including: obtaining a driver’s license or official identification card in the victim’s name
13 but with the thief’s picture; using the victim’s name and SSN to obtain government
14 benefits; or, filing a fraudulent tax return using the victim’s information. In addition,
15 identity thieves may obtain a job using the victim’s SSN, rent a house, or receive medical
16 services in the victim’s name, and may even give the victim’s personal information to
17 police during an arrest, resulting in an arrest warrant being issued in the victim’s name.¹¹

18 _____
19 States Government Accountability Office, *available at*
20 <http://www.gao.gov/new.items/d07737.pdf>.

21 ⁸ *Id.*

22 ⁹ *See Identity Theft*, Federal Trade Commission,
23 <http://www.consumer.ftc.gov/features/feature-0014-identity-theft> (last visited Sept. 8,
2015).

24 ¹⁰ The FTC defines identity theft as “a fraud committed or attempted using the
25 identifying information of another person without authority.” 17 C.F.R. § 248.201. The
26 FTC describes “identifying information” as “any name or number that may be used,
27 alone or in conjunction with any other information, to identify a specific person,”
28 including, among other things, “[n]ame, Social Security number, date of birth, official
State or government issued driver’s license or identification number, alien registration
number, government passport number, employer or taxpayer identification number.” *Id.*

¹¹ *See Warning Signs of Identity Theft*, Federal Trade Commission, *available at*
<https://www.identitytheft.gov/Warning-Signs-of-Identity-Theft> (last visited May 28,

1 50. Personal Information is such a valuable commodity to identity thieves that
2 once the information has been compromised, criminals often trade the information on the
3 “cyber black-market” for years. As a result of recent large-scale data breaches, identity
4 thieves and cyber criminals have openly posted stolen credit card numbers, SSNs, and
5 other Personal Information directly on various Internet websites making the information
6 publicly available.

7 51. There may be a time lag between when Private Information is stolen and
8 when it is used. According to the U.S. Government Accountability Office (“GAO”):
9 [L]aw enforcement officials told us that in some cases, *stolen data may be held for up to*
10 *a year or more before being used to commit identity theft*. Further, once stolen data have
11 been sold or posted on the Web, *fraudulent use of that information may continue for*
12 *years*. As a result, studies that attempt to measure the harm resulting from data breaches
13 cannot necessarily rule out all future harm.¹²

14
15 **IV. Plaintiff’s Experiences.**

16 52. Plaintiff Fred Shakib is a customer of FAFC.

17 53. Plaintiff was involved in at least five real estate transactions where FAFC
18 was the title insurer, most recently in 2019.

19 54. In order to purchase title insurance from FAFC, Plaintiff was required to
20 provide FAFC with Personal Information in exchange for an agreement with FAFC to
21 receive title insurance and to protect his Personal Information in accordance with GLB,
22 federal, state and local laws, and industry standards.

23 55. As such, Plaintiff paid FAFC for title insurance and, among other things, the
24 protection of his Personal Information.

25
26 _____
27 2019).

28 ¹² GAO, Report to Congressional Requesters, at 33 (June 2007) (italics added), *available at* <<http://www.gao.gov/new.items/d07737.pdf>> (last visited Feb. 26, 2019).

1 56. Had Plaintiff known of FAFC's substandard data security procedures and
2 methods of protecting and storing his Personal Information, he would have purchased
3 insurance elsewhere.

4 57. Because FAFC did not sufficiently protect his Personal Information,
5 Plaintiff did not receive the entirety of the services he paid for and, as a result, he paid
6 more than he otherwise would have for such services.

7 58. Additionally, Plaintiff took (and continues to take) considerable precautions
8 to protect the unauthorized dissemination of his Personal Information. Unfortunately, as
9 a result of FAFC's failure to implement its promised and paid-for security practices,
10 Plaintiff's Personal Information was disseminated without his consent and the value of
11 that information was quantifiably reduced.

12 59. As a result, Plaintiff suffered damages in (i) an amount equal to the
13 difference in value between the services paid for and the services delivered, and (ii) the
14 value of his personal data and lost property in the form of his breached and compromised
15 Personal Information. Additionally, as a result of FAFC's data breach, Plaintiff now faces
16 a substantial risk that unauthorized third parties will misuse his Personal Information.

17
18 **V. CLASS ALLEGATIONS**

19 **A. National Data Breach Class**

20 60. Plaintiff seeks relief in her individual capacity and as a representative of all
21 others who are similarly situated.

22 61. In accordance with Fed. R. Civ. P. 23(a) and (b)(2) and/or (b)(3), Plaintiff
23 seeks certification of the following Class:

24
25 All persons residing in the United States who purchased title insurance and/or
26 other products or services from FAFC and whose Personal Information was
27 exposed through FAFC's website (the "Class").
28

1 **B. Alternate Statewide Statutory Class**

2 62. Pursuant to Fed. R. Civ. P. 23(b)(1), (b)(2), and (b)(3), and in the alternative
3 to the statutory claims asserted on behalf of the National Data Breach Class, Plaintiff
4 asserts statutory claims for violation of state consumer protection statutes (Count VI) and
5 state data breach notification statutes (Count VII) on behalf of separate statewide classes,
6 defined as follows:

7 **Statewide [name of State] Statutory Classes:** All residents of [name of
8 State] whose Personal Information was maintained on FAFC's database and
9 compromised as a result of the breach announced by FAFC on or around May
10 24, 2019.

11 63. Plaintiff asserts the state consumer protection statute claims (Count VI)
12 under the consumer protection laws of the following states: Arizona, Arkansas,
13 California, Colorado, Connecticut, Delaware, Hawaii, Idaho, Illinois, Indiana, Iowa,
14 Kansas, Kentucky, Maine, Maryland, Massachusetts, Michigan, Minnesota, Montana,
15 Nebraska, New Hampshire, New Jersey, New Mexico, Nevada, New York, North
16 Carolina, North Dakota, Ohio, Oklahoma, Oregon, Pennsylvania, Rhode Island, South
17 Dakota, Texas, Utah, Vermont, Washington, West Virginia, and Wyoming.

18 64. Plaintiff asserts the state data breach notification law claims (Count VIII) on
19 behalf of separate statewide classes in and under the respective data breach statutes of the
20 following states: California, Illinois, Iowa, Louisiana, Maryland, New Hampshire, New
21 Jersey, North Carolina, South Carolina, Tennessee, Texas, Virginia, and Washington.

22 65. Excluded from the Classes and Subclass are: (1) Defendant, any entity or
23 division in which Defendant has a controlling interest, and its legal representatives,
24 officers, directors, assigns, and successors; (2) the Judge to whom this case is assigned
25 and the Judge's staff; and (3) governmental entities. Plaintiff reserve the right to amend
26 the Class definitions if discovery and further investigation reveal that the Classes should
27 be expanded, divided into further subclasses or modified in any other way.

1 **C. Certification of the Proposed Classes is Appropriate.**

2 66. Each of the proposed classes meets the certification under Fed. R. Civ. P.
3 23(a), (b)(1), (b)(2), and (b)(3).

4 67. **Numerosity:** The exact number of members of the Classes is unknown to
5 Plaintiff at this time, but on information and belief, there are approximately 855 million
6 individuals in the Class, making joinder of each individual member impracticable.
7 Ultimately, members of the Classes will be easily identified through FAFC's records.

8 68. **Commonality and Predominance:** There are many questions of law and
9 fact common to the claims of Plaintiff and the other members of the Classes, and those
10 questions predominate over any questions that may affect individual members of the
11 Classes. Common questions for the Classes include:

- 12 a. Whether Defendant failed to adequately safeguard Plaintiff's and the
13 Classes' Personal Information;
- 14 b. Whether Defendant failed to protect or otherwise keep Plaintiff's and the
15 Classes' Personal Information secure, as promised;
- 16 c. Whether Defendant's storage of Plaintiff's and the Classes' Personal
17 Information in the manner alleged violated GLB, federal, state and local
18 laws, or industry standards;
- 19 d. Whether Defendant engaged in unfair or deceptive practices by failing to
20 properly safeguard Plaintiff's and the Classes' Personal Information as
21 promised;
- 22 e. Whether Defendant violated the consumer protection statutes applicable to
23 Plaintiff and the Class;
- 24 f. Whether Defendant failed to notify Plaintiff and members of the Classes
25 about the security breach as soon as practical and without delay after the
26 breach was discovered;
- 27 g. Whether Defendant acted negligently in failing to properly safeguard
28 Plaintiff's and the Classes' Personal Information;

- 1 h. Whether Defendant's conduct described herein constitutes a breach of its
2 implied or express contracts with Plaintiff and the members of the Class;
- 3 i. Whether Defendant should retain the money paid by Plaintiff and members
4 of the Classes to protect their Personal Information; and
- 5 j. Whether Plaintiff and the members of the Classes are entitled to damages as
6 a result of Defendant's conduct.

7 69. **Typicality:** Plaintiff's claims are typical of the claims of the members of the
8 Classes. Plaintiff and the members of the Classes sustained damages as a result of
9 Defendant's uniform wrongful conduct.

10 70. **Adequacy:** Plaintiff will fairly and adequately represent and protect the
11 interests of the Classes, and have retained counsel competent and experiences in complex
12 litigation and class actions. Plaintiff has no interests antagonistic to those of the Class,
13 and Defendant has no defenses unique to Plaintiff. Plaintiff and their counsel are
14 committed to vigorously prosecuting this action on behalf of the members of the proposed
15 Classes, and have the financial resources to do so. Neither Plaintiff nor their counsel have
16 any interest adverse to those of the other members of the Class.

17 71. **Risks of Prosecuting Separate Actions:** This case is appropriate for
18 certification because prosecution of separate actions would risk either inconsistent
19 adjudications which would establish incompatible standards of conduct for Defendant or
20 would be dispositive of the interests of members of the proposed Class.

21 72. **Policies Generally Applicable to the Classes:** This class action is
22 appropriate for certification because Defendant has acted or refused to act on grounds
23 generally applicable to the Plaintiff and proposed Classes as a whole, thereby requiring
24 the Court's imposition of uniform relief to ensure compatible standards of conduct
25 towards members of the Classes, and making final injunctive relief appropriate with
26 respect to the proposed Classes as a whole. Defendant's practices challenged herein apply
27 to and affect the members of the Classes uniformly, and Plaintiff's challenge of those
28

1 practices hinges on Defendant’s conduct with respect to the proposed Classes as a whole,
2 not on individual facts or law applicable only to Plaintiff.

3 73. **Superiority:** This case is also appropriate for certification because class
4 proceedings are superior to all other available means of fair and efficient adjudication of
5 the claims of Plaintiff and the members of the Class. The injuries suffered by each
6 individual member of the Classes are relatively small in comparison to the burden and
7 expense of individual prosecution of the litigation necessitated by Defendant’s conduct.
8 Absent a class action, it would be virtually impossible for individual members of the
9 Classes to obtain effective relief from Defendant. Even if members of the Classes could
10 sustain individual litigation, it would not be preferable to a class action because individual
11 litigation would increase the delay and expense to all parties, including the Court, and
12 would require duplicative consideration of the legal and factual issues presented here. By
13 contrast, a class action presents far fewer management difficulties and provides the
14 benefits of single adjudication, economies of scale, and comprehensive supervision by a
15 single Court.

16
17 **COUNT I**
18 **Violation of California Unfair Competition Law,**
19 **Bus. & Prof. Code § 17200, *et seq.***
20 **(On behalf of Plaintiff and the National Data Breach Class**
21 **or, alternatively, the Statewide Statutory Law Classes)**

22 74. Plaintiff incorporates the allegations above as if fully set forth here.

23 75. Defendant engaged in unfair, fraudulent, and unlawful business practices in
24 violation of the Unfair Competition Law (“UCL”).

25 76. Plaintiff suffered injury in fact and lost money or property as a result of
26 Defendant’s alleged violations of the UCL.

27 77. The acts, omissions, and conduct of Defendant as alleged constitute
28 “business practices” within the meaning of the UCL.

1 78. Defendant violated the unlawful prong of the UCL by violating, *inter alia*,
2 the GLB, as alleged above, as well as state data breach laws, including Cal. Civ. Code
3 § 1798.81.

4 79. Defendant's acts, omissions, and conduct also violate the unfair prong of the
5 UCL because those acts, omissions, and conduct, as alleged herein, offended public
6 policy and constitute immoral, unethical, oppressive, and unscrupulous activities that
7 caused substantial injury, including to Plaintiff and Class members. The harm cause by
8 Defendant's conduct outweighs any potential benefits attributable to such conduct and
9 there were reasonably available alternatives to further Defendant's legitimate business
10 interests, other than Defendant's conduct described herein.

11 80. Defendant's conduct also undermines California public policy—as reflected
12 in statutes like the California's Customer Records Act, Cal. Civ. Code § 1798, *et seq.*,
13 concerning customer records—which seek to protect customer data and ensure that
14 entities who solicit or are entrusted with personal data utilize reasonable security
15 measures.

16 81. By disclosing, exposing, and/or misusing Plaintiff's and Class Members'
17 Personal Information without authorization, Defendants engaged in a fraudulent business
18 practice that is likely to deceive a reasonable consumer.

19 82. A reasonable person would not have agreed purchase title insurance or other
20 products and services from FAFC had he or she known the truth about Defendant's
21 practices alleged herein. By withholding material information about their practices,
22 Defendant was able to convince customers to provide and entrust their Personal
23 Information to Defendant. Accordingly, Defendant's conduct also was "fraudulent"
24 within the meaning of the UCL.

25 83. As a result of Defendant's violations of the UCL, Plaintiff and Class
26 Members are entitled to injunctive relief.

27 84. As a result of Defendant's violations of the UCL, Plaintiff and Class
28 members have suffered injury in fact and lost money or property, as detailed above.

1 Plaintiff request that the Court issue sufficient equitable relief to restore Class Members
2 to the position they would have been in had Defendant not engaged in unfair competition.

3 **COUNT II**

4 **Negligence**

5 **(On behalf of Plaintiff and the National Data Breach Class**
6 **or, alternatively, the Statewide Common Law Classes)**

7 85. Plaintiff incorporates the foregoing allegations as if fully set forth herein.

8 86. FAFC required Plaintiff and Class members to submit non-public Personal
9 Information in order to obtain coverage.

10 87. By collecting and storing this data, FAFC had a duty of care to use
11 reasonable means to secure and safeguard this Personal Information, to prevent disclosure
12 of the information, and to guard the information from theft. FAFC's duty included a
13 responsibility to implement a process by which it could detect a breach of its security
14 systems in a reasonably expeditious period of time and to give prompt notice in the case
15 of a data breach.

16 88. FAFC owed a duty to Plaintiff and members of the Classes to provide
17 security consistent with industry standards and the other requirements discussed herein,
18 and to ensure that its systems and networks—and the personnel responsible for them—
19 adequately protected its customers' Personal Information.

20 89. FAFC further assumed the duty to implement reasonable security measures
21 as a result of its general conduct, internal policies and procedures, in which FAFC states
22 that it "will maintain appropriate facilities and systems to protect against unauthorized
23 access to and corruption of the data we maintain." Through these statements, FAFC
24 specifically assumed the duty to comply with industry standards and GLB in protecting
25 confidential information.

26 90. FAFC's duty to use reasonable security measures arose as a result of the
27 special relationship that existed between FAFC and the Plaintiff and the members of the
28 Class. The special relationship arose because Plaintiff and the members of the Classes

1 entrusted Defendant with their confidential data, as part of the title insurance process.
2 Only FAFC was in a position to ensure that its systems were sufficient to protect against
3 the harm to Plaintiff and the members of the Classes from a data breach.

4 91. FAFC's duty to use reasonable security measures also arose under GLB,
5 pursuant to which FAFC was required to protect the security, confidentiality, and
6 integrity of customer information by developing a comprehensive written information
7 security program that contains reasonable administrative, technical, and physical
8 safeguards.

9 92. In addition, FAFC had a duty to use reasonable security measures under
10 Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits "unfair
11 . . . practices in or affecting commerce," including, as interpreted and enforced by the
12 FTC, the unfair practice of failing to use reasonable measures to protect confidential data.

13 93. FAFC's duty to use reasonable care in protecting confidential data arose not
14 only as a result of the common law and the statutes and regulations described above, but
15 also because it was bound by, and had committed to comply with, industry standards for
16 the protection of confidential Personal Information.

17 94. FAFC breached its common law, statutory and other duties—and thus, was
18 negligent—by failing to use reasonable measures to protect consumers' confidential data
19 and by failing to provide timely notice of the at-issue breach. The specific negligent acts
20 and omissions committed by FAFC include, but are not limited to, the following:

- 21 (a) failing to adopt, implement, and maintain adequate security measures to safeguard
22 Plaintiff's and proposed members of the Classes' confidential data;
23 (b) failing to adequately monitor the security of its networks;
24 (c) allowing unauthorized access to Plaintiff's and the proposed members of the
25 Classes' confidential data;
26 (d) failing to recognize in a timely manner that Plaintiff's and proposed members of
27 the Classes' confidential data had been compromised; and
28

1 (e) failing to warn Plaintiff and the members of the proposed Classes in a timely
2 manner that their Personal Information had been compromised.

3 95. It was foreseeable that FAFC failure to use reasonable measures to protect
4 confidential data and to provide timely notice of a breach of such data would result in
5 injury to Plaintiff and the members of the Class. Further, the breach of security,
6 unauthorized access, and resulting injury to Plaintiff and the members of the Classes were
7 reasonably foreseeable.

8 96. It was therefore foreseeable that the failure to adequately safeguard
9 confidential data would result in one or more of the following injuries to Plaintiff and the
10 members of the proposed Class: ongoing, imminent, certainly impending threat of
11 identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm;
12 actual identity theft crimes, fraud, and abuse, resulting in monetary loss and economic
13 harm; loss of the confidentiality of the stolen confidential data; the illegal sale of the
14 compromised data on the deep web black market; expenses and/or time spent on credit
15 monitoring and identity theft insurance; time spent scrutinizing bank statements, credit
16 card statements, and credit reports; expenses and/or time spent initiating fraud alerts;
17 decreased credit scores and ratings; lost work time; and other economic and non-
18 economic harm.

19 97. Accordingly, Plaintiff, on behalf of themselves and members of the Classes
20 seek an order declaring that Defendant's conduct constitutes negligence, and awarding
21 them damages in an amount to be determined at trial.

22
23 **COUNT III**
24 **Breach of Express Contract**
25 **(On behalf of Plaintiff and the National Data Breach Class)**

26 98. Plaintiff incorporates the foregoing allegations as if fully set forth here.

27 99. Plaintiff and members of the Classes entered into valid and enforceable
28 contracts with Defendant whereby it promised to provide title insurance and data

1 protection services to them. Plaintiff and members of the Classes agreed to, among other
2 things, pay money for such services.

3 100. Both aspects of Plaintiff's and the members of the Classes' agreements with
4 Defendant (*i.e.*, the provision of title insurance and data protection services) were
5 material.

6 101. In its Privacy Information, public statements, and other written
7 understandings, Defendant expressly promised Plaintiff and members of the Classes to
8 safeguard and protect the confidentiality of their Personal Information in accordance with
9 GLB regulations, federal, state and/or local laws, and industry standards.

10 102. Defendant promised to comply with all GLB regulations, federal, state
11 and/or local laws, and industry standards to make sure that Plaintiff's and the members
12 of the Classes' Personal Information was protected.

13 103. These contracts required that Defendant protect Plaintiff's and the members
14 of the Classes' Personal Information and to prevent unauthorized access to such
15 information.

16 104. Unfortunately, Defendant did not safeguard Plaintiff's and the Class
17 members' Personal Information. Specifically, Defendant did not comply with its
18 promises to abide by GLB, federal, state and/or local laws, or industry standards.

19 105. The failure to meet these promises and obligations constitutes a breach of
20 express contract.

21 106. Because Defendant allowed unauthorized access to Plaintiff's and the
22 members of the Classes' Personal Information and otherwise failed to safeguard it as
23 promised, Defendant breached its contracts with Plaintiff and members of the Class.

24 107. A meeting of the minds occurred, as Plaintiff and members of the Classes
25 agreed to, among other things, provide Defendant with their accurate and complete
26 information (including their Personal Information) and to pay Defendant in exchange for
27 its agreement to, among other things, protect their Personal Information.

28

1 108. Defendant breached these contracts by failing to implement (or adequately
2 implement) sufficient security measures to protect Plaintiff's and the members of the
3 Classes' Personal Information.

4 109. Defendant's failure to fulfill its data security and management promises
5 resulted in Plaintiff and members of the Classes receiving title insurance that was of less
6 value than they paid for (*i.e.*, title insurance coverage without adequate data security and
7 management practices).

8 110. Stated otherwise, because Plaintiff and members of the Classes paid for
9 privacy protections (as part of, among other things, their premiums) they did not
10 receive—even though such protections were a material part of their contracts with
11 Defendant—the full benefit of their bargain.

12 111. As a result of Defendant's conduct, Plaintiff and members of the Classes
13 have suffered actual damages in an amount equal to the difference in the value of the
14 secure title insurance they paid for and the insecure title insurance they received.

15 112. Accordingly, Plaintiff, on behalf of themselves and the other members of
16 the Classes seek an order declaring that Defendant's conduct constitutes breach of express
17 contract, and awarding them damages in an amount to be determined at trial.

18
19 **COUNT IV**
20 **Breach of Implied Contract**
21 ***(In the Alternative to Breach of Express Contract)***
22 **(On behalf of Plaintiff and the National Data Breach Class)**

23 113. Plaintiff incorporates the foregoing allegations as if fully set forth here.

24 114. In order to benefit from Defendant's title insurance coverage, Plaintiff and
25 members of the Classes provided Defendant with their Personal Information.

26 115. By providing that Personal Information, and upon Defendant's acceptance
27 of such information, Plaintiff and members of the Class, on the one hand, and Defendant,
28 on the other, entered into implied contracts whereby Defendant was obligated to take
reasonable steps to secure and safeguard that information.

1 116. Under those implied contracts, Defendant was further obligated to provide
2 Plaintiff and members of the Classes with prompt and sufficient notice of any and all
3 unauthorized access and/or theft of their Personal Information.

4 117. Without such implied contracts, Plaintiff and members of the Classes would
5 not have provided their Personal Information to Defendant.

6 118. As described throughout, Defendant did not take reasonable steps to
7 safeguard Plaintiff's and members of the Classes' Personal Information.

8 119. Because Defendant allowed unauthorized access to Plaintiff's and the
9 members of the Classes' Personal Information and failed to take reasonable steps to
10 safeguard that information, Defendant breached its implied contracts with Plaintiff and
11 members of the Class.

12 120. Defendant's failure to fulfill its data security and management promises
13 resulted in Plaintiff and members of the Classes receiving title insurance that was of less
14 value than they paid for (*i.e.*, title insurance coverage without adequate data security and
15 management practices).

16 121. Stated otherwise, because Plaintiff and members of the Classes paid for
17 privacy protections (as part of, among other things, their premiums) they did not
18 receive—even though such protections were a material part of their contracts with
19 Defendant—the full benefit of their bargain.

20 122. As a result of Defendant's conduct, Plaintiff and members of the Classes
21 have suffered actual damages in an amount equal to the difference in the value of the
22 secure title insurance they paid for and the insecure title insurance they received.

23 123. Accordingly, Plaintiff, on behalf of themselves and members of the Classes
24 seek an order declaring that Defendant's conduct constitutes breach of implied contract,
25 and awarding them damages in an amount to be determined at trial.

26
27
28

COUNT V
Violation of State Consumer Protection Laws
(In the Alternative to Count I)
(On behalf of Plaintiff and the Statewide Statutory Classes)

124. Plaintiff incorporates the foregoing allegations as if fully set forth here.

125. The consumer protection laws listed below were enacted to protect consumers by promoting fair competition in commercial markets for goods and services. Specifically, they prohibit unlawful, unfair, deceptive, or fraudulent business acts or practices, including the employment of any deception, fraud, false pretense, false promise, or misrepresentation, or the concealment, suppression, or omission of any material fact.

126. As described herein, Defendant engaged in unlawful, unfair, and deceptive business acts or practices.

127. Through its Privacy Information, public statements, and other written understandings, Defendant promised that it would, among other things, safeguard and protect Personal Information in accordance with GLB regulations, federal, state and/or local laws, and industry standards.

128. Defendant's privacy and data-security promises were, in fact, false. As described in Sections II–III above, Defendant did not implement adequate security protocols to prevent unauthorized access to Personal Information, maintain an adequate electronic security system to prevent data breaches, or employ industry standard and commercially viable measures to mitigate the risks of any data breach or otherwise comply with GLB data security requirements. Thus, Defendant's representations regarding its data-security protocols were false when made.

129. As described throughout this Complaint, Defendant was responsible for securing Plaintiff's and the Statewide Statutory Classes' Personal Information. As it was responsible for creating, overseeing, maintaining, or otherwise implementing its own data security practices, Defendant knew (or should have known) that it was not adequately

1 protecting Plaintiff's or the Statewide Statutory Classes' Personal Information. Prior to
2 the May 24, 2019, neither Plaintiff, members of the Statewide Statutory Classes, nor the
3 general public knew that Defendant was not implementing adequate data security and
4 privacy protocols. By representing that it could and would protect their Personal
5 Information, when it did not in fact do so, Defendant actively concealed its true security
6 practices from Plaintiff and the Statewide Statutory Classes.

7 130. Consumers—like Plaintiff and members of the Statewide Statutory Classes
8 —value their privacy. Services (including title insurance) that offer greater data security
9 protections are more valuable to consumers than those with substandard security
10 practices. As such, consumers will, if given the choice between two otherwise identical
11 services, choose one with adequate security practices over one with substandard security
12 practices.

13 131. Because of this consumer preference for data security, a title insurance
14 company safeguarding and protecting Personal Information in accordance with GLB
15 regulations, federal, state and/or local laws, and industry standards commands a higher
16 market price for its coverage than a provider with substandard security.

17 132. Defendant's failure to disclose its substandard security practices
18 substantially injured the public because it caused millions of consumers to enter into
19 transactions they otherwise would not have, and because it compromised the integrity of
20 Plaintiff's and the Statewide Statutory Classes' Personal Information. Further,
21 Defendant's use of substandard security did not create any benefits sufficient to outweigh
22 the harm it caused.

23 133. Defendant's unfair acts or practices occurred in its trade or business and
24 have injured a substantial portion of the public. Defendant's general course of conduct is
25 injurious to the public interest, and such acts are ongoing and/or have a substantial
26 likelihood of being repeated inasmuch as the long-lasting harmful effects of its
27 misconduct may last for years (*e.g.*, affected individuals could experience identity theft
28

1 years later). As a direct and proximate result of Defendant's unfair acts, Plaintiff and
2 members of the Statewide Statutory Classes have suffered and will suffer actual injuries.

3 134. Accordingly, Defendant's misrepresentations and/or omissions regarding its
4 data security and privacy-related practices constitutes unlawful, deceptive, and unfair
5 conduct in violation of the following State-specific consumer protection laws:

- 6 a. Arizona Consumer Fraud Act, Ariz. Rev. Stat. § 44-1522;
- 7 b. Arkansas Deceptive Trade Practices Act, Ark. Code Ann. §§ 4-88-107–108;
- 8 c. California Consumer Legal Remedies Act, Cal. Civ. Code §§ 1750, *et seq.*;
- 9 d. California Unfair Competition Law, Cal. Bus. & Prof. Code §§ 17200, *et*
10 *seq.*;
- 11 e. Colorado Consumer Protection Act, Colo. Rev. Stat. § 6-1-105(1);
- 12 f. Connecticut Unfair Trade Practices Act, Conn. Gen. Stat. §§ 42-110b, *et*
13 *seq.*;
- 14 g. Delaware Consumer Fraud Act, Del. Code Ann. tit. 6, §§ 2513, *et seq.*;
- 15 h. Delaware Deceptive Trade Practices Act, Del. Code Ann. Tit. 6, §§ 2532(5)
16 and (7);
- 17 i. Hawaii Consumer Protection Act, Haw. Rev. Stat. Ann. §§ 480-2(a), *et seq.*;
- 18 j. Hawaii Deceptive Trade Practices Act, Haw. Rev. Stat. Ann. §§ 481A-
19 3(a)(5), (7), and (12), *et seq.*;
- 20 k. Idaho Consumer Protection Act, Idaho Code Ann. §§ 48-603, *et seq.*;
- 21 l. Illinois Consumer Fraud and Deceptive Business Practices Act, 815 Ill.
22 Comp. Stat. Ann. §§ 505/2, *et seq.*;
- 23 m. Illinois Uniform Deceptive Trade Practices Act, 815 Ill. Comp. Stat. Ann.
24 §§ 510/2, *et seq.*;
- 25 n. Indiana Deceptive Consumer Sales Act, Ind. Code Ann. § 24-5-0.5-3(a),
26 (b)(1), and (2), *et seq.*;
- 27 o. Iowa Consumer Fraud Act, Iowa Code §§ 714H.3 and 714H.5, *et seq.*;
- 28

- 1 p. Kansas Consumer Protection Act, Kan. Stat. Ann. § 50-626(a) and
2 (b)(1)(A), (D) and (b)(3), *et seq.*;
- 3 q. Kentucky Consumer Protection Act, Ky. Rev. Stat. Ann. § 367.170(1) and
4 (2), *et seq.*;
- 5 r. Maine Unfair Trade Practices Act, Me. Rev. Stat. Ann. tit. 5, § 207, *et seq.*;
- 6 s. Maine Uniform Deceptive Trade Practices Act, Me. Rev. Stat. Ann. tit. 10,
7 § 1212(1)(E) and (G), *et seq.*;
- 8 t. Maryland Consumer Protection Act, Md. Code Ann. Com. Law, § 13-
9 301(1), (2)(i)-(ii),(iv), (5)(i), and (9)(i), *et seq.*;
- 10 u. Massachusetts Consumer Protection Act, Mass. Gen. Laws ch. 93A, § 2(a),
11 *et seq.*;
- 12 v. Michigan Consumer Protection Act, Mich. Comp. Laws Ann. §
13 445.903(1)(c), (e), (s), and (cc), *et seq.*;
- 14 w. Minnesota Uniform Deceptive Trade Practices Act, Minn. Stat. § 325D.44,
15 subd. 1(5), (7), and (13), *et seq.*;
- 16 x. Minnesota Consumer Fraud Act, Minn. Stat. § 325F.69, subd. 1, and Minn.
17 Stat. § 8.31, subd. 3(A);
- 18 y. Montana Unfair Trade Practices and Consumer Protection Act, Mont. Code
19 Ann. §§ 30-14-103;
- 20 z. Nebraska Consumer Protection Act, Neb. Rev. Stat. Ann. § 59-1602;
- 21 aa. Nebraska Uniform Deceptive Trade Practices Act, Neb. Rev. Stat. Ann. §
22 87-302(A)(5) and (7);
- 23 bb. New Hampshire Consumer Protection Act, N.H. Rev. Stat. Ann. § 358-
24 A:2(V) and (VII);
- 25 cc. New Jersey Consumer Fraud Act, N.J. Stat. Ann. § 56:8-2;
- 26 dd. New Mexico Unfair Practices Act, N.M. Stat. Ann. §§ 57-12-2(D)(5)(7),
27 (14), and 57-12-3;
- 28

- 1 ee. Nevada Deceptive Trade Practices Act, Nev. Rev. Stat. Ann. § 598.0915(5)
- 2 and (7);
- 3 ff. New York Business Law, N.Y. Gen. Bus. Law § 349(A);
- 4 gg. North Carolina Unfair Trade Practices Act, N.C. Gen. Stat. Ann. § 75-
- 5 1.1(A);
- 6 hh. North Dakota Unlawful Sales or Advertising Practices Law, N.D. Cent.
- 7 Code § 51-15-02;
- 8 ii. Ohio Consumer Sales Practices Act, Ohio Rev. Code Ann. § 1345.02(A) and
- 9 (B)(1) and (2);
- 10 jj. Oklahoma Consumer Protection Act, Okla. Stat. Ann. § 753(5), (7), and
- 11 (20);
- 12 kk. Oklahoma Deceptive Trade Practices Act, Okla. Stat. Ann. tit. 78, §
- 13 53(A)(5) and (7);
- 14 ll. Oregon Unfair Trade Practices Act, Or. Rev. Stat. § 646.608(1)(E), (G), and
- 15 (U);
- 16 mm. Pennsylvania Unfair Trade Practices and Consumer Protection Law, 73 Pa.
- 17 Stat. Ann. §§ 201-2(4)(V), (VII), (XXI), and 201-3;
- 18 nn. Rhode Island Deceptive Trade Practices Act, R.I. Gen. Laws § 6-13.1-
- 19 1(6)(V), (VII), (XII), (XIII), and (XIV);
- 20 oo. South Dakota Deceptive Trade Practices Act and Consumer Protection Act,
- 21 S.D. Codified Laws § 37-24-6(1);
- 22 pp. Texas Deceptive Trade Practices-Consumer Protection Act, Tex. Bus. &
- 23 Com. Code Ann. § 17.46(A), (B)(5) and (7);
- 24 qq. Utah Consumer Sales Practices Act, Utah Code Ann. § 13-11-4(1) and
- 25 (2)(A), (B), and (I);
- 26 rr. Vermont Consumer Fraud Act, 9 Vt. Stat. Ann. Tit. 9, § 2453(A);
- 27 ss. Washington Consumer Protection Act, Wash. Rev. Code RCW §§
- 28 19.86.010, *et seq.*;

- 1 tt. West Virginia Consumer Credit and Protection Act, W. Va. Code Ann. §
2 46A-6-104; and
3 uu. Wyoming Consumer Protection Act, Wyo. Stat. Ann. § 40-12-105(a), (i),
4 (iii), and (xv).

5 135. As a result of Defendant's conduct, Plaintiff and members of the Statewide
6 Statutory Classes have suffered actual damages, including from the lost value of their
7 personal data and lost property in the form of their breached and compromised Personal
8 Information (which is of great value to third parties); ongoing, imminent, certainly
9 impending threat of identity theft crimes, fraud, and abuse, resulting in monetary loss and
10 economic harm; actual identity theft crimes, fraud, and abuse, resulting in monetary loss
11 and economic harm; loss of the confidentiality of the stolen confidential data; the illegal
12 sale of the compromised data on the deep web black market; expenses and/or time spent
13 on credit monitoring and identity theft insurance; time spent scrutinizing bank statements,
14 credit card statements, and credit reports; expenses and/or time spent initiating fraud
15 alerts; decreased credit scores and ratings; lost work time; and other economic and non-
16 economic harm.

17 136. Accordingly, Plaintiff, on behalf of themselves and members of the
18 Statewide Statutory Classes, seek to enjoin further violation and recover actual damages
19 (and treble damages where applicable).

20 137. With respect to injunctive relief, Plaintiff, on behalf of themselves and
21 members of the Statewide Statutory Classes, seek an Order requiring FAFC to: (1) engage
22 third-party security auditors/penetration testers as well as internal security personnel to
23 conduct testing, including simulated attacks, penetration tests, and audits on FAFC's
24 systems on a periodic basis, and ordering FAFC to promptly correct any problems or
25 issues detected by such third-party security auditors; (2) engage third-party security
26 auditors and internal personnel to run automated security monitoring; (3) audit, test, and
27 train its security personnel regarding any new or modified procedures; (4) segment data
28 by, among other things, creating firewalls and access controls so that if one area of

1 FAFC's network is compromised, hackers cannot gain access to other portions of FAFC's
2 systems; (5) purge, delete, and destroy in a reasonably secure manner Personal
3 Information not necessary for its provisions of services; (6) conduct regular database
4 scanning and securing checks; (7) routinely and continually conduct internal training and
5 education to inform internal security personnel how to identify and contain a breach when
6 it occurs and what to do in response to a breach; and (8) meaningfully educate all Class
7 members about the threats they face as a result of the loss of their confidential financial,
8 personal, and health information to third parties, as well as the steps affected individuals
9 must take to protect themselves.

10
11 **COUNT VI**
12 **Violation of State Data Breach Notification Laws**
13 **(On behalf of Plaintiff and the Statewide Statutory Classes)**

14 138. Plaintiff incorporates the foregoing allegations as if fully set forth here.

15 139. The data breach notification laws listed below were enacted to protect (or at
16 least mitigate damage for) consumers from the consequences associated with data
17 breaches. In relevant part, those laws require that businesses that maintain consumer data
18 (including Personal Information) notify the owner of any breach of that data in the most
19 expedient time and manner possible and without unreasonable delay.

20 140. The data breach described in Section II resulted in a breach of Plaintiff's and
21 the Statewide Statutory members of the Classes' Personal Information.

22 141. Defendant failed to disclose the breach of Plaintiff's and the Statewide
23 Statutory members of the Classes' Personal Information in the most expedient time
24 possible inasmuch as, after discovering the breach, it waited months before notifying all
25 affected individuals. Defendant unreasonably delayed informing Plaintiff and members
26 of the Statewide Statutory Class about the data breach after it knew or should have known
27 that the data breach had occurred.

1 142. Defendant's failure to provide timely notice of the data breach violated the
2 following State-specific data breach notification laws:

- 3 a. Cal. Civ. Code § 1798.80, *et seq.*;
- 4 b. Ill. Comp. Stat. Ann. 530/10, *et seq.*;
- 5 c. Iowa Code Ann. § 715C.2, *et seq.*;
- 6 d. La. Rev. Stat. Ann. § 51:3074, *et seq.*;
- 7 e. Md. Code Ann., Commercial Law § 14-3504, *et seq.*;
- 8 f. N.H. Rev. Stat. Ann. § 359-C:20, *et seq.*;
- 9 g. N.J. Stat. Ann. § 56:8-163, *et seq.*;
- 10 h. N.C. Gen. Stat. Ann. § 75-65, *et seq.*;
- 11 i. S.C. Code § 39-1-90, *et seq.*;
- 12 j. Tenn. Code Ann. § 47-18-2107, *et seq.*;
- 13 k. Tex. Bus. & Com. Code Ann. § 521.053, *et seq.*; and
- 14 l. Va. Code Ann. § 18.2-186.6, *et seq.*;

15 143. As a result of Defendant's conduct, Plaintiff and members of the Statewide
16 Statutory Class have suffered actual damages, including from the lost value of their
17 personal data and lost property in the form of their breached and compromised Personal
18 Information (which is of great value to third parties); ongoing, imminent, certainly
19 impending threat of identity theft crimes, fraud, and abuse, resulting in monetary loss and
20 economic harm; actual identity theft crimes, fraud, and abuse, resulting in monetary loss
21 and economic harm; loss of the confidentiality of the stolen confidential data; the illegal
22 sale of the compromised data on the deep web black market; expenses and/or time spent
23 on credit monitoring and identity theft insurance; time spent scrutinizing bank statements,
24 credit card statements, and credit reports; expenses and/or time spent initiating fraud
25 alerts; decreased credit scores and ratings; lost work time; and other economic and non-
26 economic harm.

27 144. Accordingly, Plaintiff, on behalf of themselves and members of the
28 Statewide Statutory Class, seek all remedies available under their state data breach

1 statute, including but not limited to (a) damages suffered by Plaintiff and the Statewide
2 Statutory Class members as alleged above, (b) equitable relief, including injunctive relief,
3 and (c) reasonable attorney fees and costs, as provided by law.

4
5 **REQUEST FOR RELIEF**

6 Plaintiff, on behalf of themselves and the Classes, respectfully request that this Court
7 enter an Order:

8 A. Certifying this case as a class action on behalf of Plaintiff and the Classes
9 defined above, appointing Plaintiff as representatives of their respective Classes, and
10 appointing their counsel as Class Counsel;

11 B. Awarding injunctive and other equitable relief as is necessary to protect the
12 interests of the Classes, including (i) an order prohibiting FAFC from engaging in the
13 wrongful and unlawful acts described herein, and (ii) requiring FAFC to protect all data
14 collected through the course of its business in accordance with GLB regulations, industry
15 standards, and federal, state and/or local laws; (iii) requiring FAFC to engage third-party
16 security auditors/penetration testers as well as internal security personnel to conduct
17 testing, including simulated attacks, penetration tests, and audits on FAFC's systems on
18 a periodic basis, and ordering FAFC to promptly correct any problems or issues detected
19 by such third-party security auditors; (iv) requiring FAFC to engage third-party security
20 auditors and internal personnel to run automated security monitoring; (v) requiring FAFC
21 to audit, test, and train its security personnel regarding any new or modified procedures;
22 (vi) requiring FAFC to segment data by, among other things, creating firewalls and access
23 controls so that if one area of FAFC's network is compromised, hackers cannot gain
24 access to other portions of FAFC's systems; (vii) requiring FAFC to purge, delete, and
25 destroy in a reasonably secure manner Personal Information not necessary for its
26 provisions of services; (viii) requiring FAFC to conduct regular database scanning and
27 securing checks; (ix) requiring FAFC to routinely and continually conduct internal
28 training and education to inform internal security personnel how to identify and contain

1 a breach when it occurs and what to do in response to a breach; and (x) requiring FAFC
2 to meaningfully educate all class members about the threats they face as a result of the
3 loss of their confidential Personal Information to third parties, as well as the steps affected
4 individuals must take to protect themselves.

5 C. Awarding damages to Plaintiff and the Classes in an amount to be
6 determined at trial;

7 D. Awarding restitution to Plaintiff and the Classes in an amount to be
8 determined at trial;

9 E. Awarding Plaintiff and the Classes their reasonable litigation expenses and
10 attorneys' fees;

11 F. Awarding Plaintiff and the Classes pre- and post-judgment interest, to the
12 extent allowable; and

13 G. Awarding such other and further relief as equity and justice may require.
14

15 **JURY DEMAND**

16 Plaintiff request a trial by jury.
17

18 Respectfully submitted,
19 **AHDOOT & WOLFSON, PC**

20 Dated: May 28, 2019

/s/ Tina Wolfson

Tina Wolfson, SBN 174806
twolfson@ahdootwolfson.com

Theodore Maya, SBN 223242
tmaya@ahdootwolfson.com

Alex R. Straus, SBN 321366
astraus@ahdootwolfson.com

AHDOOT & WOLFSON, PC

10728 Lindbrook Drive

Los Angeles, CA 90024

27 Tel: 310-474-9111

28 Fax: 310-474-8585

ClassAction.org

This complaint is part of ClassAction.org's searchable class action lawsuit database and can be found in this post: [First American Financial Corp. Sued Over Allegedly 'Reckless' Customer Data Exposure](#)
