

FILED
Superior Court Of California,
Sacramento
09/20/2022
jeroute
By Deputy
Case Number:
34-2021-00300923

1 Michael F. Ram, Esq. (SBN 104805)
2 **MORGAN & MORGAN**
3 **COMPLEX LITIGATION GROUP**
4 711 Van Ness Avenue, Suite 500
5 San Francisco, CA 94102
6 Telephone: (415) 358-6913
7 Facsimile: (415) 358-6923
8 Email: mram@forthepeople.com

9 M. Anderson Berry, Esq. (SBN 262879)
10 Gregory Haroutunian, Esq. (SBN 330263)
11 **CLAYEO C. ARNOLD,**
12 **A PROFESSIONAL LAW CORP.**
13 865 Howe Avenue
14 Sacramento, CA 95825
15 Telephone: (916) 239-4778
16 Facsimile: (916) 924-1829
17 Email: aberry@justice4you.com;
18 gharoutunian@justice4you.com

19 John A. Yanchunis, Esq.
20 (*Pro Hac Vice*)
21 Ryan D. Maxey, Esq.
22 (*Pro Hac Vice application pending*)
23 **MORGAN & MORGAN**
24 **COMPLEX LITIGATION GROUP**
25 201 N. Franklin Street, 7th Floor
26 Tampa, Florida 33602
27 Telephone: (813) 223-5505
28 Email: jyanchunis@ForThePeople.com;
rmaxey@ForThePeople.com

Kevin S. Hannon, Esq.
THE HANNON LAW FIRM, LLC
1641 North Downing Street
Denver, Colorado 80218
Telephone: (303) 861-8800
Email: khannon@hannonlaw.com

Attorneys for Plaintiff and the Putative Class

BY FAX

SUPERIOR COURT OF THE STATE OF CALIFORNIA
COUNTY OF SACRAMENTO

RICHARD ARCHIBEQUE,
on behalf of himself and all others similarly
situated,

Plaintiff,

vs.

FPI MANAGEMENT, INC.,

Defendant.

Case No. 34-2021-00300923-CU-MT-GDS

Designated Complex and Assigned for All
Purposes to: Hon. Jill H. Talley; Dept. 25

**FIRST AMENDED CLASS ACTION
COMPLAINT**

Complaint Filed: May 17, 2021
Trial Date: None Set

Plaintiff Richard Archibeque ("Plaintiff"), individually and on behalf of all others similarly situated ("Class Members"), brings this Amended Class Action Complaint against FPI Management, Inc. ("Defendant" or "FPI"), and alleges, upon personal knowledge as to his own actions and his counsels' investigations, and upon information and belief as to all other matters, as follows:

I. INTRODUCTION

1. Plaintiff brings this class action against Defendant for its failure to properly secure and safeguard sensitive information that residents of properties that Defendant managed entrusted to it, including, without limitation, name, address, date of birth, Social Security number, driver's license number or other government identification card number, passport number, tax identification number, financial account information, online credentials, digital signature, and/or payment card information (collectively, "personally identifiable information" or "PII") as well as medical information (collectively, "protected health information" or "PHI").¹

¹ Personally identifiable information generally incorporates information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information. 2 CFR § 200.79. At a minimum, it includes all information that on its face expressly identifies an individual. PII also is generally defined to include certain identifiers that do not on their face name an individual, but that are considered to be particularly sensitive and/or valuable if in the wrong hands (for example, Social Security number, passport number, driver's license number, financial account number).

1 2. According to Defendant's website, it "is a privately owned, exclusive third-party,
2 multifamily property manager."² Its "client list includes institutional investors, international real
3 estate investment firms, financial institutions, multifamily development builders, private investors,
4 City, County, and State agencies."³

5 3. Plaintiff and Class Members, as residents of the properties that Defendant manages,
6 entrust Defendant with an extensive amount of their PII and PHI. Defendant retains this
7 information on computer hardware—even after the relationship ends. Defendant asserts that it
8 understands the importance of protecting such information.

9 4. On or before August 14, 2020, Defendant learned that an unauthorized actor gained
10 access to certain of Defendant's systems and thereby accessed or acquired the PII and PHI of
11 Plaintiff and Class Members without authorization (the "Data Breach").

12 5. On or before August 14, 2020, Defendant learned that, during the Data Breach, the
13 unauthorized actor gained access to files that contained the PII and PHI of Plaintiff and Class
14 Members, including, but not limited to, name, address, date of birth, Social Security number,
15 driver's license number or other government identification card number, passport number, tax
16 identification number, financial account information, online credentials, digital signature, payment
17 card information, and / or medical information, as well as other personal information.

18 6. By obtaining, collecting, using, and deriving a benefit from Plaintiff's and Class
19 Members' PII and PHI, Defendant assumed legal and equitable duties to those individuals.

20 7. The exposed PII and PHI of Plaintiff and Class Members can be sold on the dark
21 web. Hackers can access and then offer for sale the unencrypted, unredacted PII and PHI to
22 criminals. Plaintiff and Class Members face a lifetime risk of identity theft, which is heightened
23 here by the loss of Social Security numbers.

24 8. This PII and PHI was compromised due to Defendant's negligent and/or careless
25 acts and omissions and the failure to protect the PII and PHI of Plaintiff and Class Members.

26
27 ² See <https://fpimgt.com> (last visited May 3, 2021).

28 ³ *Id.*

9. Plaintiff brings this action on behalf of all persons whose PII and PHI was compromised as a result of Defendant's failure to: (i) adequately protect the PII and PHI of Plaintiff and Class Members; (ii) warn Plaintiff and Class Members of its inadequate information security practices; and (iii) avoid sharing the PII and PHI of Plaintiff and Class Members without adequate safeguards. Defendant's conduct amounts to negligence and violates federal and state statutes.

10. Plaintiff and Class Members have suffered injury as a result of Defendant's conduct. These injuries include: (i) lost or diminished value of PII and PHI; (ii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII and PHI; (iii) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, including but not limited to lost time, and significantly (iv) the continued and certainly an increased risk to their PII and PHI, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) may remain backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII and PHI.

11. Defendant disregarded the rights of Plaintiff and Class Members by intentionally, willfully, recklessly, or negligently failing to take and implement adequate and reasonable measures to ensure that Plaintiff's and Class Members' PII and PHI was safeguarded, failing to take available steps to prevent an unauthorized disclosure of data, and failing to follow applicable, required, and appropriate protocols, policies, and procedures regarding the encryption of data, even for internal use. As the result, the PII and PHI of Plaintiff and Class Members was compromised through disclosure to an unknown and unauthorized third party. Plaintiff and Class Members have a continuing interest in ensuring that their information is and remains safe, and they should be entitled to injunctive and other equitable relief.

II. PARTIES

12. Plaintiff Richard Archibeque is a citizen of California residing in San Joaquin County, California.

1 13. Defendant FPI Management, Inc. is a California corporation with its principal place
2 of business in Sacramento County, California.

3 14. The true names and capacities of persons or entities, whether individual, corporate,
4 associate, or otherwise, who may be responsible for some of the claims alleged herein are currently
5 unknown to Plaintiff. Plaintiff will seek leave of court to amend this complaint to reflect the true
6 names and capacities of such other responsible parties when their identities become known.

7 15. All of Plaintiff's claims stated herein are asserted against Defendant and any of its
8 owners, predecessors, successors, subsidiaries, agents and/or assigns.

9
10 **III. JURISDICTION AND VENUE**

11 16. This Court has jurisdiction over this matter pursuant to the California Constitution,
12 Article VI, § 10 and California Code of Civil Procedure ("CCP") § 410.10, because Defendant
13 transacted business and committed the acts alleged in California.

14 17. Venue is appropriate in Sacramento County because Defendant did and is doing
15 business in Sacramento County and gathered the PII and PHI of Plaintiff and Class Members from
16 Defendant's headquarters in Sacramento County, California.

17 **IV. FACTUAL ALLEGATIONS**

18 **A. Background**

19 18. Defendant collected and stored some of Plaintiff's and Class Members most
20 sensitive and confidential information, including, but not limited to, name, address, date of birth,
21 Social Security number, driver's license number or other government identification card number,
22 passport number, tax identification number, financial account information, online credentials,
23 digital signature, payment card information, and / or medical information, as well as other personal
24 information, which include information that is static, does not change, and can be used to commit
25 myriad financial crimes.

26 19. Plaintiff and Class Members relied on this sophisticated Defendant to keep their PII
27 and PHI confidential and securely maintained, to use this information for business purposes only,
28

1 and to make only authorized disclosures of this information. Plaintiff and Class Members demand
2 security to safeguard their PII and PHI.

3 20. Defendant had a duty to adopt reasonable measures to protect Plaintiff's and Class
4 Members' PII and PHI from involuntary disclosure to third parties.

5 **B. The Data Breach**

6 21. On or about April 15, 2021, Defendant informed various state attorneys general that
7 it was subject to the Data Breach. In its sample breach notices filed with the attorneys general,
8 Defendant reported the Data Breach as follows:

9 **What Happened:** On August 14, 2020, FPI learned that it had experienced a data
10 security incident that disrupted access to certain of its systems. Upon discovering
11 this incident, FPI took immediate steps to secure its systems prior to restoration.
12 In addition, FPI retained independent cybersecurity experts to conduct an
13 investigation in order to determine what happened. FPI learned that an
14 unauthorized third party had gained access to certain FPI systems and that
15 personal information stored on such systems was accessed or acquired without
16 authorization. On March 3, 2021, following a thorough review of potentially
17 impacted information, FPI learned that your personal information may have been
18 accessed or acquired without authorization as a result of this incident. FPI then
19 worked diligently to provide notification of this incident.

16 Please note that FPI is not aware of the misuse of any potentially impacted
17 information in connection with this incident, and that FPI is notifying potentially
18 impacted individuals out of an abundance of caution.

18 **What Information Was Involved:** The incident may have impacted your name,
19 address, date of birth, Social Security number, driver's license number or other
20 government identification card number, passport number, tax identification
21 number, financial account information, online credentials, digital signature,
22 payment card information, and / or medical information.

22 **What We Are Doing:** When FPI learned of this incident, FPI immediately began
23 containment, mitigation, and restoration efforts. As set forth above, FPI also
24 launched an investigation and engaged independent cybersecurity experts to
25 determine what happened and whether sensitive information was impacted. In
26 addition, FPI implemented additional security measures to further harden its
27 digital environment in an effort to prevent a similar event from occurring in the
28 future. Finally, FPI reported this incident to the Federal Bureau of Investigation
and will provide any assistance needed to hold the perpetrators accountable.⁴

⁴ Ex. 1 (Sample breach notice filed with California Attorney General).

1 22. Defendant admitted in the sample breach notices that an unauthorized party gained
2 access to files that contained sensitive information about Plaintiff and Class Members, including
3 names, Social Security numbers, driver's license information, dates of birth, home addresses,
4 financial account information, payment card information, and other information.

5 23. In response to the Data Breach, Defendant claims that it "immediately began
6 containment, mitigation, and restoration efforts" and "implemented additional security measures to
7 further harden its digital environment in an effort to prevent a similar event from occurring in the
8 future."⁵ However, the details of the root cause of the Data Breach, the vulnerabilities exploited,
9 and the remedial measures undertaken to ensure a breach does not occur again have not been shared
10 with regulators or Plaintiff and Class Members, who retain a vested interest in ensuring that their
11 information remains protected.

12 24. Plaintiff's and Class Members' unencrypted information may end up for sale on the
13 dark web, or simply fall into the hands of companies that will use the detailed PII and PHI for
14 targeted marketing without the approval of Plaintiff and Class Members. Unauthorized individuals
15 can easily access the PII and PHI of Plaintiff and Class Members.

16 25. Defendant did not use reasonable security procedures and practices appropriate to
17 the nature of the sensitive, unencrypted information it was maintaining for Plaintiff and Class
18 Members, causing their PII and PHI to be exposed.

19 **C. Defendant Acquires, Collects and Stores Plaintiff's and Class Members' PII**
20 **and PHI**

21 26. Defendant acquired, collected, and stored Plaintiff's and Class Members' PII and
22 PHI.

23 27. As a condition of its relationships with Plaintiff and Class Members, Defendant
24 required that Plaintiff and Class Members entrust Defendant with highly confidential PII and PHI.

25 ///

26 ///

27 _____
28 ⁵ *Id.*

1 28. By obtaining, collecting, and storing the PII and PHI of Plaintiff and Class Members,
2 Defendant assumed legal and equitable duties and knew or should have known that it was
3 responsible for protecting the PII and PHI from disclosure.

4 29. Plaintiff and Class Members have taken reasonable steps to maintain the
5 confidentiality of their PII and PHI and relied on Defendant to keep their PII and PHI confidential
6 and securely maintained, to use this information for business purposes only, and to make only
7 authorized disclosures of this information.

8 **D. Securing PII and PHI and Preventing Breaches**

9 30. Defendant could have prevented this Data Breach by properly securing and
10 encrypting the PII and PHI of Plaintiff and Class Members. Alternatively, Defendant could have
11 destroyed the data, especially decade-old data from former residents.

12 31. Defendant's negligence in safeguarding the PII and PHI of Plaintiff and Class
13 Members is exacerbated by the repeated warnings and alerts directed to protecting and securing
14 sensitive data.

15 32. Despite the prevalence of public announcements of data breach and data security
16 compromises, Defendant failed to take appropriate steps to protect the PII and PHI of Plaintiff and
17 Class Members from being compromised.

18 33. The Federal Trade Commission ("FTC") defines identity theft as "a fraud committed
19 or attempted using the identifying information of another person without authority."⁶ The FTC
20 describes "identifying information" as "any name or number that may be used, alone or in
21 conjunction with any other information, to identify a specific person," including, among other
22 things, "[n]ame, Social Security number, date of birth, official State or government issued driver's
23 license or identification number, alien registration number, government passport number, employer
24 or taxpayer identification number."⁷

25 ///

26
27 ⁶ 17 C.F.R. § 248.201 (2013).

28 ⁷ *Id.*

1 34. The ramifications of Defendant's failure to keep secure the PII and PHI of Plaintiff
2 and Class Members are long lasting and severe. Once PII and PHI is stolen, particularly Social
3 Security numbers, fraudulent use of that information and damage to victims may continue for years.

4 **E. Value of Personal Identifiable Information**

5 35. The PII of individuals remains of high value to criminals, as evidenced by the prices
6 they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity
7 credentials. For example, personal information can be sold at a price ranging from \$40 to \$200,
8 and bank details have a price range of \$50 to \$200.⁸ Experian reports that a stolen credit or debit
9 card number can sell for \$5 to \$110 on the dark web.⁹ Criminals can also purchase access to entire
10 company data breaches from \$900 to \$4,500.¹⁰

11 36. Social Security numbers, for example, are among the worst kind of personal
12 information to have stolen because they may be put to a variety of fraudulent uses and are difficult
13 for an individual to change. The Social Security Administration stresses that the loss of an
14 individual's Social Security number, as is the case here, can lead to identity theft and extensive
15 financial fraud:

16 A dishonest person who has your Social Security number can use it to get other
17 personal information about you. Identity thieves can use your number and your
18 good credit to apply for more credit in your name. Then, they use the credit cards
19 and don't pay the bills, it damages your credit. You may not find out that
20 someone is using your number until you're turned down for credit, or you begin
21 to get calls from unknown creditors demanding payment for items you never
22 bought. Someone illegally using your Social Security number and assuming your
23 identity can cause a lot of problems.¹¹

23 ⁸ *Your personal data is for sale on the dark web. Here's how much it costs*, Digital Trends, Oct. 16, 2019, available at:
24 <https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/> (last accessed Apr.
25 5, 2021).

25 ⁹ *Here's How Much Your Personal Information Is Selling for on the Dark Web*, Experian, Dec. 6, 2017, available at:
26 [https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-](https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/)
27 [web/](https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/) (last accessed Apr. 5, 2021).

26 ¹⁰ *In the Dark*, VPNOverview, 2019, available at: <https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/>
27 (last accessed Apr. 5, 2021).

27 ¹¹ Social Security Administration, *Identity Theft and Your Social Security Number*, available at:
28 <https://www.ssa.gov/pubs/EN-05-10064.pdf> (last accessed Apr. 5, 2021).

1 37. What is more, it is no easy task to change or cancel a stolen Social Security number.
2 An individual cannot obtain a new Social Security number without significant paperwork and
3 evidence of actual misuse. In other words, preventive action to defend against the possibility of
4 misuse of a Social Security number is not permitted; an individual must show evidence of actual,
5 ongoing fraud activity to obtain a new number.

6 38. Even then, a new Social Security number may not be effective. According to Julie
7 Ferguson of the Identity Theft Resource Center, “The credit bureaus and banks are able to link the
8 new number very quickly to the old number, so all of that old bad information is quickly inherited
9 into the new Social Security number.”¹²

10 39. Based on the foregoing, the information compromised in the Data Breach is
11 significantly more valuable than the loss of, for example, credit card information in a retailer data
12 breach because, there, victims can cancel or close credit and debit card accounts. The information
13 compromised in this Data Breach is impossible to “close” and difficult, if not impossible, to
14 change—name, Social Security number, and potentially date of birth.

15 40. This data demands a much higher price on the black market. Martin Walter, senior
16 director at cybersecurity firm RedSeal, explained, “Compared to credit card information, personally
17 identifiable information and Social Security numbers are worth more than 10x on the black
18 market.”¹³

19 41. Among other forms of fraud, identity thieves may obtain driver’s licenses,
20 government benefits, medical services, and housing or even give false information to police.

21 42. The PII and PHI of Plaintiff and Class Members was taken by hackers to engage in
22 identity theft or and or to sell it to other criminals who will purchase the PII and PHI for that
23 purpose. The fraudulent activity resulting from the Data Breach may not come to light for years.

24
25 ¹² Bryan Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR (Feb. 9, 2015), available
26 at: <http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millionsworrying-about-identity-theft> (last accessed Apr. 5, 2021).

27 ¹³ Time Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, IT World,
28 (Feb. 6, 2015), available at: <https://www.networkworld.com/article/2880366/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html> (last accessed Apr. 5, 2021).

1 43. There may be a time lag between when harm occurs versus when it is discovered,
2 and also between when PII and PHI is stolen and when it is used. According to the U.S. Government
3 Accountability Office (“GAO”), which conducted a study regarding data breaches:

4 [L]aw enforcement officials told us that in some cases, stolen data may be held
5 for up to a year or more before being used to commit identity theft. Further, once
6 stolen data have been sold or posted on the Web, fraudulent use of that
7 information may continue for years. As a result, studies that attempt to measure
8 the harm resulting from data breaches cannot necessarily rule out all future
9 harm.¹⁴

10 44. At all relevant times, Defendant knew, or reasonably should have known, of the
11 importance of safeguarding the PII and PHI of Plaintiff and Class Members, including Social
12 Security numbers and/or dates of birth, and of the foreseeable consequences that would occur if the
13 PII and PHI was compromised, including, specifically, the significant costs that would be imposed
14 on Plaintiff and Class Members a result.

15 45. Plaintiff and Class Members now face years of constant surveillance of their
16 financial and personal records, monitoring, and loss of rights. Plaintiff and Class Members are
17 incurring and will continue to incur such damages in addition to any fraudulent use of their PII and
18 PHI.

19 46. Defendant was, or should have been, fully aware of the unique type and the
20 significant volume of data stored on and/or shared on its system, amounting to more than 20,000
21 individuals detailed, personal information and, thus, the significant number of individuals who
22 would be harmed by the exposure of the unencrypted data.

23 47. To date, Defendant has offered Plaintiff and Class Members only one year of identity
24 theft protection services through a single provider, Experian. The offered service is inadequate to
25 protect Plaintiff and Class Members from the threats they face for years to come, particularly in
26 light of the PII and PHI at issue here.

27 ///

28 ¹⁴ Report to Congressional Requesters, GAO, at 29 (June 2007), available at: <https://www.gao.gov/products/gao-07-737> (last accessed Apr. 5, 2021).

1 48. The injuries to Plaintiff and Class Members were directly and proximately caused
2 by Defendant's failure to implement or maintain adequate data security measures for the PII and
3 PHI of Plaintiff and Class Members.

4 ***Plaintiff Richard Archibeque's Experience***

5 49. In August 2016, Plaintiff Archibeque began residing in one of the residential
6 properties that Defendant managed.

7 50. On or around April 14, 2021, Plaintiff Archibeque received a Notice of Data Breach
8 from Defendant.¹⁵

9 51. As a result of the Data Breach, Plaintiff Archibeque spent time dealing with the
10 consequences of the Data Breach, which includes time spent on the telephone and sorting through
11 his unsolicited emails, verifying the legitimacy of the Data Breach, exploring credit monitoring and
12 identity theft insurance options, and self-monitoring his accounts. This time has been lost forever
13 and cannot be recaptured.

14 52. Additionally, Plaintiff Archibeque is very careful about sharing his PII and PHI. He
15 has never knowingly transmitted unencrypted PII or PHI over the internet or any other unsecured
16 source.

17 53. Plaintiff Archibeque stores any documents containing his PII and PHI in a safe and
18 secure location. Moreover, he diligently chooses unique usernames and passwords for his few
19 online accounts.

20 54. Plaintiff Archibeque suffered actual injury in the form of damages to and diminution
21 in the value of his PII and PHI—a form of intangible property that Plaintiff Archibeque entrusted
22 to Defendant for the purpose of residing in a property managed by Defendant, which was
23 compromised in and as a result of the Data Breach.

24 55. Plaintiff Archibeque suffered lost time, annoyance, interference, and inconvenience
25 as a result of the Data Breach and has anxiety and increased concerns for the loss of his privacy.

26 ///

27 _____
28 ¹⁵ Ex. 2.

1 56. Plaintiff Archibeque has suffered imminent and impending injury arising from the
2 substantially increased risk of fraud, identity theft, and misuse resulting from his PII and PHI,
3 especially his Social Security number, in combination with his name, being placed in the hands of
4 unauthorized third parties and possibly criminals.

5 57. Plaintiff Archibeque has a continuing interest in ensuring that his PII and PHI,
6 which, upon information and belief, remain backed up in Defendant's possession, is protected and
7 safeguarded from future breaches.

8 **V. CLASS ALLEGATIONS**

9 58. Plaintiff brings this nationwide class action on behalf of himself and on behalf of all
10 others similarly situated pursuant to Code of Civil Procedure § 382, Civil Code § 1781, and other
11 applicable law.

12 59. The Nationwide Class that Plaintiff seeks to represent is defined as follows:

13 All individuals residing in the United States whose PII or PHI was accessed or
14 acquired without authorization during the data breach referenced in the Notice of
15 Data Breach that Defendant sent to Plaintiff on or around April 14, 2021 (the
 "Nationwide Class").

16 60. In the alternative to claims asserted on behalf of the Nationwide Class, Plaintiff
17 asserts claims on behalf of a separate subclass, defined as follows:

18 All individuals residing in California whose PII or PHI was accessed or acquired
19 without authorization during the data breach referenced in the Notice of Data
20 Breach that Defendant sent to Plaintiff on or around April 14, 2021 (the
 "California Class").

21 61. Excluded from the Classes are the following individuals and/or entities: Defendant
22 and Defendant's parents, subsidiaries, affiliates, officers and directors, and any entity in which
23 Defendant has a controlling interest; all individuals who make a timely election to be excluded from
24 this proceeding using the correct protocol for opting out; any and all federal, state or local
25 governments, including but not limited to their departments, agencies, divisions, bureaus, boards,
26 sections, groups, counsels and/or subdivisions; and all judges assigned to hear any aspect of this
27 litigation, as well as their immediate family members.
28

1 62. Plaintiff reserves the right to modify or amend the definition of the proposed classes
2 before the Court determines whether certification is appropriate.

3 63. This action is brought and may be maintained as a class action because there is a
4 well-defined community of interest among many persons who comprise a readily ascertainable
5 class. A well-defined community of interest exists to warrant class wide relief because Plaintiff
6 and all members of the Nationwide Class were subjected to the same wrongful practices by
7 Defendant, entitling them to the same relief.

8 64. The Nationwide Class is so numerous that individual joinder of its members is
9 impracticable. While the exact number of Class Members is unknown to Plaintiff at this time,
10 Plaintiff is informed and believes that there are at least tens of thousands of Class Members.
11 Defendant advised the Attorney General of Maine that the Data Breach affected 21,417 individuals.

12 65. Common questions of law and fact exist as to members of the Nationwide Class and
13 predominate over any questions which affect only individual members of the Class. These common
14 questions include, but are not limited to:

- 15 a. Whether and to what extent Defendant had a duty to protect the PII and PHI of Plaintiff
16 and Class Members;
- 17 b. Whether Defendant had a duty not to disclose the PII and PHI of Plaintiff and Class
18 Members to unauthorized third parties;
- 19 c. Whether Defendant had a duty not to use the PII and PHI of Plaintiff and Class Members
20 for non-business purposes;
- 21 d. Whether Defendant failed to adequately safeguard the PII and PHI of Plaintiff and Class
22 Members;
- 23 e. Whether and when Defendant actually learned of the Data Breach;
- 24 f. Whether Defendant adequately, promptly, and accurately informed Plaintiff and Class
25 Members that their PII and PHI had been compromised;
- 26 g. Whether Defendant violated the law by failing to promptly notify Plaintiff and Class
27 Members that their PII and PHI had been compromised;

- 1 h. Whether Defendant failed to implement and maintain reasonable security procedures
2 and practices appropriate to the nature and scope of the information compromised in the
3 Data Breach;
- 4 i. Whether Defendant adequately addressed and fixed the vulnerabilities which permitted
5 the Data Breach to occur;
- 6 j. Whether Defendant engaged in unfair, unlawful, or deceptive practices by failing to
7 safeguard the PII and PHI of Plaintiff and Class Members;
- 8 k. Whether Plaintiff and Class Members are entitled to actual, damages, and/or statutory
9 damages as a result of Defendant's wrongful conduct;
- 10 l. Whether Plaintiff and Class Members are entitled to restitution as a result of Defendant's
11 wrongful conduct; and
- 12 m. Whether Plaintiff and Class Members are entitled to injunctive relief to redress the
13 imminent and currently ongoing harm faced as a result of the Data Breach.

14 66. Plaintiff is a member of the Classes he seeks to represent, and his claims and injuries
15 are typical of the claims and injuries of the other Class Members.

16 67. Plaintiff will adequately and fairly protect the interests of other Class Members.
17 Plaintiff has no interests adverse to the interests of absent Class Members. Plaintiff is represented
18 by legal counsel with substantial experience in class action litigation. The interests of Class
19 Members will be fairly and adequately protected by Plaintiff and his counsel.

20 68. Defendant has acted or refused to act on grounds that apply generally to the Class
21 Members, so that final injunctive relief or corresponding declaratory relief is appropriate respecting
22 the Class as a whole.

23 69. A class action is superior to other available means for fair and efficient adjudication
24 of the claims of the Class and would be beneficial for the parties and the court. Class action
25 treatment will allow a large number of similarly situated persons to prosecute their common claims
26 in a single forum, simultaneously, efficiently, and without the unnecessary duplication of effort and
27 expense that numerous individual actions would require. The amounts owed to the many individual
28

1 Class Members are likely to be relatively small, and the burden and expense of individual litigation
2 would make it difficult or impossible for individual members of the class to seek and obtain relief.
3 A class action will serve an important public interest by permitting such individuals to effectively
4 pursue recovery of the sums owed to them. Further, class litigation prevents the potential for
5 inconsistent or contradictory judgments raised by individual litigation. Plaintiff is unaware of any
6 difficulties that are likely to be encountered in the management of this action that would preclude
7 its maintenance as a class action.

8 **COUNT I**

9 **Negligence**

10 **(On Behalf of Plaintiff and the Nationwide Class)**

11 70. Plaintiff and the Nationwide Class re-allege and incorporate by reference herein all
12 the allegations contained in paragraphs 1 through 69.

13 71. Plaintiff and the Nationwide Class provided and entrusted Defendant with certain
14 PII and PHI, including their full names, addresses, dates of birth, Social Security numbers, driver's
15 license numbers or other government identification card numbers, passport numbers, tax
16 identification numbers, financial account information, online credentials, digital signatures,
17 payment card information, and/or medical information, as well as other personal information.

18 72. Plaintiff and the Nationwide Class entrusted their PII and PHI to Defendant on the
19 premise and the understanding that Defendant would safeguard their information, use their PII and
20 PHI for business purposes only, and/or not disclose their PII and PHI to unauthorized third parties.

21 73. Defendant has full knowledge of the sensitivity of the PII and PHI and the types of
22 harm that Plaintiff and the Nationwide Class could and would suffer if the PII and PHI were
23 wrongfully disclosed.

24 74. Defendant knew or reasonably should have known that the failure to exercise due
25 care in the collecting, storing, and using of the PII and PHI of Plaintiff and the Nationwide Class
26 involved an unreasonable risk of harm to Plaintiff and the Nationwide Class, even if the harm
27 occurred through the criminal acts of a third party.

1 75. Defendant had a duty to exercise reasonable care in safeguarding, securing, and
2 protecting such information from being compromised, lost, stolen, misused, and/or disclosed to
3 unauthorized parties. This duty includes, among other things, designing, maintaining, and testing
4 Defendant's security protocols to ensure that the PII and PHI of Plaintiff and the Nationwide Class
5 in Defendant's possession was adequately secured and protected.

6 76. Defendant also had a duty to exercise appropriate clearinghouse practices to remove
7 PII and PHI it was no longer required to retain pursuant to regulations, including that of former
8 residents of properties that Defendant managed.

9 77. Defendant also had a duty to have procedures in place to detect and prevent the
10 improper access and misuse of the PII and PHI of Plaintiff and the Nationwide Class.

11 78. Defendant's duty to use reasonable security measures arose as a result of the special
12 relationship that existed between Defendant and Plaintiff and the Nationwide Class. That special
13 relationship arose because Plaintiff and the Nationwide Class entrusted Defendant with their
14 confidential PII and PHI, a necessary part of their relationships with Defendant.

15 79. Defendant was subject to an "independent duty," untethered to any contract between
16 Defendant and Plaintiff or the Nationwide Class.

17 80. A breach of security, unauthorized access, and resulting injury to Plaintiff and the
18 Nationwide Class was reasonably foreseeable, particularly in light of Defendant's inadequate
19 security practices.

20 81. Plaintiff and the Nationwide Class were the foreseeable and probable victims of any
21 inadequate security practices and procedures. Defendant knew or should have known of the
22 inherent risks in collecting and storing the PII and PHI of Plaintiff and the Nationwide Class, the
23 critical importance of providing adequate security of that PII and PHI, and the necessity for
24 encrypting PII and PHI stored on Defendant's systems.

25 82. Defendant's own conduct created a foreseeable risk of harm to Plaintiff and the
26 Nationwide Class. Defendant's misconduct included, but was not limited to, its failure to take the
27 steps and opportunities to prevent the Data Breach as set forth herein. Defendant's misconduct also
28

1 included its decisions not to comply with industry standards for the safekeeping of the PII and PHI
2 of Plaintiff and the Nationwide Class, including basic encryption techniques freely available to
3 Defendant.

4 83. Plaintiff and the Nationwide Class had no ability to protect their PII and PHI that
5 was in, and possibly remains in, Defendant's possession.

6 84. Defendant was in a position to protect against the harm suffered by Plaintiff and the
7 Nationwide Class as a result of the Data Breach.

8 85. Defendant had and continues to have a duty to adequately disclose that the PII and
9 PHI of Plaintiff and the Nationwide Class within Defendant's possession might have been
10 compromised, how it was compromised, and precisely the types of data that were compromised and
11 when. Such notice was necessary to allow Plaintiff and the Nationwide Class to take steps to
12 prevent, mitigate, and repair any identity theft and the fraudulent use of their PII and PHI by third
13 parties.

14 86. Defendant had a duty to employ proper procedures to prevent the unauthorized
15 dissemination of the PII and PHI of Plaintiff and the Nationwide Class.

16 87. Defendant has admitted that the PII and PHI of Plaintiff and the Nationwide Class
17 was wrongfully lost and disclosed to unauthorized third persons as a result of the Data Breach.

18 88. Defendant, through its actions and/or omissions, unlawfully breached its duties to
19 Plaintiff and the Nationwide Class by failing to implement industry protocols and exercise
20 reasonable care in protecting and safeguarding the PII and PHI of Plaintiff and the Nationwide
21 Class during the time the PII and PHI was within Defendant's possession or control.

22 89. Defendant improperly and inadequately safeguarded the PII and PHI of Plaintiff and
23 the Nationwide Class in deviation of standard industry rules, regulations, and practices at the time
24 of the Data Breach.

25 90. Defendant failed to heed industry warnings and alerts to provide adequate
26 safeguards to protect the PII and PHI of Plaintiff and the Nationwide Class in the face of increased
27 risk of theft.

1 91. Defendant, through its actions and/or omissions, unlawfully breached its duty to
2 Plaintiff and the Nationwide Class by failing to have appropriate procedures in place to detect and
3 prevent dissemination of their PII and PHI.

4 92. Defendant breached its duty to exercise appropriate clearinghouse practices by
5 failing to remove PII and PHI it was no longer required to retain pursuant to regulations, including
6 PII and PHI of former residents.

7 93. Defendant, through its actions and/or omissions, unlawfully breached its duty to
8 adequately and timely disclose to Plaintiff and the Nationwide Class the existence and scope of the
9 Data Breach.

10 94. But for Defendant's wrongful and negligent breach of duties owed to Plaintiff and
11 the Nationwide Class, the PII and PHI of Plaintiff and the Nationwide Class would not have been
12 compromised.

13 95. There is a close causal connection between Defendant's failure to implement
14 security measures to protect the PII and PHI of Plaintiff and the Nationwide Class and the harm, or
15 risk of imminent harm, suffered by Plaintiff and the Nationwide Class. The PII and PHI of Plaintiff
16 and the Nationwide Class was lost and accessed as the proximate result of Defendant's failure to
17 exercise reasonable care in safeguarding such PII and PHI by adopting, implementing, and
18 maintaining appropriate security measures.

19 96. Additionally, Section 5 of the FTC Act prohibits "unfair...practices in or affecting
20 commerce," including, as interpreted, and enforced by the FTC, the unfair act or practice by
21 businesses, such as Defendant, of failing to use reasonable measures to protect PII and PHI. The
22 FTC publications and orders described also form part of the basis of Defendant's duty in this regard.

23 97. Defendant violated Section 5 of the FTC Act by failing to use reasonable measures
24 to protect PII and PHI and not complying with applicable industry standards, as described in detail
25 herein. Defendant's conduct was particularly unreasonable given the nature and amount of PII and
26 PHI it obtained and stored and the foreseeable consequences of the immense damages that would
27 result to Plaintiff and the Nationwide Class.

1 98. Defendant's violation of Section 5 of the FTC Act constitutes negligence *per se*.

2 99. Plaintiff and the Nationwide Class are within the class of persons that the FTC Act
3 was intended to protect.

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

8 101. As a direct and proximate result of Defendant's negligence and negligence *per se*,
9 Plaintiff and the Nationwide Class have suffered and will suffer injury, including but not limited
10 to: (i) actual identity theft; (ii) the loss of the opportunity of how their PII and PHI is used; (iii) the
11 compromise, publication, and/or theft of their PII and PHI; (iv) out-of-pocket expenses associated
12 with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use
13 of their PII; (v) lost opportunity costs associated with effort expended and the loss of productivity
14 addressing and attempting to mitigate the actual and future consequences of the Data Breach,
15 including but not limited to efforts spent researching how to prevent, detect, contest, and recover
16 from tax fraud and identity theft; (vi) costs associated with placing freezes on credit reports; (vii)
17 the continued risk to their PII and PHI, which remain in Defendant's possession and are subject to
18 further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate
19 measures to protect the PII and PHI of Plaintiff and the Nationwide Class; and (viii) future costs in
20 terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the
21 impact of the PII and PHI compromised as a result of the Data Breach for the remainder of the lives
22 of Plaintiff and the Nationwide Class.

23 102. As a direct and proximate result of Defendant's negligence and negligence *per se*,
24 Plaintiff and the Nationwide Class have suffered and will continue to suffer other forms of injury
25 and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other
26 economic and non-economic losses.

27 ///

103. Additionally, as a direct and proximate result of Defendant's negligence and negligence *per se*, Plaintiff and the Nationwide Class have suffered and will suffer the continued risks of exposure of their PII and PHI, which remain in Defendant's possession and are subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII and PHI in its continued possession.

COUNT II

Breach of Written Contract
(On Behalf of Plaintiff and the Nationwide Class)

104. Plaintiff and the Nationwide Class re-allege and incorporate by reference herein all the allegations contained in paragraphs 1 through 69.

105. Defendant required Plaintiff and the Nationwide Class to provide and entrust their name, address, date of birth, Social Security number, driver's license number or other government identification card number, passport number, tax identification number, financial account information, online credentials, digital signature, payment card information, medical information, and/or other personal information, as a condition of residing in properties that Defendant managed.

106. Defendant's "CCPA Policy" provides, in part, as follows:

Information Security and Data Privacy Practice

FPI Management follows the **NIST CyberSecurity Framework** (National Institute of Standards and Technology) in setting our security policies and security operations along with using encryption protocols for data in transit and at rest in our systems. Although no information transmitted across the internet can be guaranteed to be secure, we follow data security best practices to encrypt sensitive data prior to sending it and while storing it in our systems. We take the privacy and security of personal information seriously and require ongoing training and testing for all FPI Management employees on data privacy.¹⁶

107. Defendant's CCPA Policy was a contract, or part of a contract, between Defendant and Plaintiff and Class Members.

¹⁶ Ex. 3 (emphasis in original).

108. Plaintiff and the Nationwide Class fully performed their obligations under the contract with Defendant.

109. Defendant breached its contract with Plaintiff and Class Members by (a) failing to follow the NIST Cybersecurity Framework in setting its security policies and security operations, (b) failing to use encryption protocols for the PII and PHI of Plaintiff and Class Members when in transit and at rest in Defendant's systems, and (c) failing to follow data security best practices to encrypt the PII and PHI of Plaintiff and Class Members prior to sending it and while storing it on Defendant's systems.

110. As a direct and proximate result of Defendant's above-described breach of contract, Plaintiff and the Nationwide Class have suffered (and will continue to suffer) ongoing, imminent, and impending threat of identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; loss of the confidentiality of the stolen confidential data; the illegal sale of the compromised data on the dark web; expenses and/or time spent on credit monitoring and identity theft insurance; time spent scrutinizing bank statements, credit card statements, and credit reports; expenses and/or time spent initiating fraud alerts, decreased credit scores and ratings; lost work time; and other economic and non-economic harm.

111. As a result of Defendant's breach of contract, Plaintiff and the Nationwide Class are entitled to recover actual damages as well as nominal damages.

COUNT III

Breach of Implied Contract (Alternatively to Count II)
(On Behalf of Plaintiff and the Nationwide Class)

112. Plaintiff and the Nationwide Class re-allege and incorporate by reference herein all the allegations contained in paragraphs 1 through 69.

113. Defendant required Plaintiff and the Nationwide Class to provide and entrust their name, address, date of birth, Social Security number, driver's license number or other government identification card number, passport number, tax identification number, financial account

1 information, online credentials, digital signature, payment card information, medical information,
2 and/or other personal information, as a condition of residing in properties that Defendant managed.

3 114. As a condition of being residing in properties that Defendant managed, Plaintiff and
4 the Nationwide Class provided and entrusted their personal information. In so doing, Plaintiff and
5 the Nationwide Class entered into implied contracts with Defendant by which Defendant agreed to
6 safeguard and protect such information, to keep such information secure and confidential, and to
7 timely and accurately notify Plaintiff and the Nationwide Class if their data had been breached and
8 compromised or stolen.

9 115. Plaintiff and the Nationwide Class fully performed their obligations under the
10 implied contracts with Defendant.

11 116. Defendant breached the implied contracts it made with Plaintiff and the Nationwide
12 Class by failing to safeguard and protect their personal and financial information and by failing to
13 provide timely and accurate notice to them that personal and financial information was
14 compromised as a result of the data breach.

15 117. As a direct and proximate result of Defendant's above-described breach of implied
16 contract, Plaintiff and the Nationwide Class have suffered (and will continue to suffer) ongoing,
17 imminent, and impending threat of identity theft crimes, fraud, and abuse, resulting in monetary
18 loss and economic harm; actual identity theft crimes, fraud, and abuse, resulting in monetary loss
19 and economic harm; loss of the confidentiality of the stolen confidential data; the illegal sale of the
20 compromised data on the dark web; expenses and/or time spent on credit monitoring and identity
21 theft insurance; time spent scrutinizing bank statements, credit card statements, and credit reports;
22 expenses and/or time spent initiating fraud alerts, decreased credit scores and ratings; lost work
23 time; and other economic and non-economic harm.

24 118. As a result of Defendant's breach of implied contract, Plaintiff and the Nationwide
25 Class are entitled to recover actual damages as well as nominal damages.

26 ///

27 ///

COUNT IV

**Invasion of Privacy
(On Behalf of Plaintiff and the Nationwide Class)**

119. Plaintiff and the Nationwide Class re-allege and incorporate by reference herein all the allegations contained in paragraphs 1 through 69.

120. Plaintiff and the Nationwide Class had a legitimate expectation of privacy to their PII and PHI and were entitled to the protection of this information against disclosure to unauthorized third parties.

121. Defendant owed a duty to its current and former residents, including Plaintiff and the Nationwide Class, to keep their PII and PHI contained as a part thereof, confidential.

122. Defendant failed to protect and released to unknown and unauthorized third parties the PII and PHI of Plaintiff and the Nationwide Class.

123. Defendant allowed unauthorized and unknown third parties access to and examination of the PII and PHI of Plaintiff and the Nationwide Class, by way of Defendant's failure to protect the PII and PHI.

124. The unauthorized release to, custody of, and examination by unauthorized third parties of the PII and PHI of Plaintiff and the Nationwide Class is highly offensive to a reasonable person.

125. The intrusion was into a place or thing, which was private and is entitled to be private. Plaintiff and the Nationwide Class disclosed their PII and PHI to Defendant as part of Plaintiff's and the Nationwide Class's relationships with Defendant, but privately with an intention that the PII and PHI would be kept confidential and would be protected from unauthorized disclosure. Plaintiff and the Nationwide Class were reasonable in their belief that such information would be kept private and would not be disclosed without their authorization.

126. The Data Breach at the hands of Defendant constitutes an intentional interference with Plaintiff's and the Nationwide Class's interest in solitude or seclusion, either as to their persons

1 or as to their private affairs or concerns, of a kind that would be highly offensive to a reasonable
2 person.

3 127. Defendant acted with a knowing state of mind when it permitted the Data Breach to
4 occur because it was with actual knowledge that its information security practices were inadequate
5 and insufficient.

6 128. Because Defendant acted with this knowing state of mind, it had notice and knew
7 the inadequate and insufficient information security practices would cause injury and harm to
8 Plaintiff and the Nationwide Class.

9 129. As a proximate result of the above acts and omissions of Defendant, the PII and PHI
10 of Plaintiff and the Nationwide Class was disclosed to third parties without authorization, causing
11 Plaintiff and the Nationwide Class to suffer damages.

12 130. Unless and until enjoined, and restrained by order of this Court, Defendant's
13 wrongful conduct will continue to cause great and irreparable injury to Plaintiff and the Nationwide
14 Class in that the PII and PHI maintained by Defendant can be viewed, distributed, and used by
15 unauthorized persons for years to come. Plaintiff and the Nationwide Class have no adequate
16 remedy at law for the injuries in that a judgment for monetary damages will not end the invasion of
17 privacy for Plaintiff and the Nationwide Class.

18 **COUNT V**

19 **Breach of Confidence**
20 **(On Behalf of Plaintiff and the Nationwide Class)**

21 131. Plaintiff and the Nationwide Class re-allege and incorporate by reference herein all
22 the allegations contained in paragraphs 1 through 69.

23 132. At all times during Plaintiff's and the Nationwide Class's interactions with
24 Defendant, Defendant was fully aware of the confidential and sensitive nature of Plaintiff's and the
25 Nationwide Class's PII and PHI that Plaintiff and the Nationwide Class provided to Defendant.

26 133. As alleged herein and above, Defendant's relationship with Plaintiff and the
27 Nationwide Class was governed by terms and expectations that Plaintiff's and the Nationwide
28

1 Class's PII and PHI would be collected, stored, and protected in confidence, and would not be
2 disclosed to unauthorized third parties.

3 134. Plaintiff and the Nationwide Class provided their PII and PHI to Defendant with the
4 explicit and implicit understandings that Defendant would protect and not permit the PII and PHI
5 to be disseminated to any unauthorized third parties.

6 135. Plaintiff and the Nationwide Class also provided their PII and PHI to Defendant with
7 the explicit and implicit understandings that Defendant would take precautions to protect that PII
8 and PHI from unauthorized disclosure.

9 136. Defendant voluntarily received in confidence the PII and PHI of Plaintiff and the
10 Nationwide Class with the understanding that PII and PHI would not be disclosed or disseminated
11 to the public or any unauthorized third parties.

12 137. Due to Defendant's failure to prevent and avoid the Data Breach from occurring, the
13 PII and PHI of Plaintiff and the Nationwide Class was disclosed and misappropriated to
14 unauthorized third parties beyond Plaintiff's and the Nationwide Class's confidence, and without
15 their express permission.

16 138. As a direct and proximate cause of Defendant's actions and/or omissions, Plaintiff
17 and the Nationwide Class have suffered damages.

18 139. But for Defendant's disclosure of Plaintiff's and the Nationwide Class's PII and PHI
19 in violation of the parties' understanding of confidence, their PII and PHI would not have been
20 compromised, stolen, viewed, accessed, and used by unauthorized third parties. The Data Breach
21 was the direct and legal cause of the theft of Plaintiff's and the Nationwide Class's PII and PHI as
22 well as the resulting damages.

23 140. The injury and harm Plaintiff and the Nationwide Class suffered was the reasonably
24 foreseeable result of Defendant's unauthorized disclosure of Plaintiff's and the Nationwide Class's
25 PII and PHI. Defendant knew or should have known its methods of accepting and securing
26 Plaintiff's and the Nationwide Class's PII and PHI was inadequate as it relates to, at the very least,
27
28

1 securing servers and other equipment containing Plaintiff's and the Nationwide Class's PII and
2 PHI.

3 141. As a direct and proximate result of Defendant's breach of its confidence with
4 Plaintiff and the Nationwide Class, Plaintiff and the Nationwide Class have suffered and will suffer
5 injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity how their
6 PII and PHI is used; (iii) the compromise, publication, and/or theft of their PII and PHI; (iv) out-
7 of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax
8 fraud, and/or unauthorized use of their PII and PHI; (v) lost opportunity costs associated with effort
9 expended and the loss of productivity addressing and attempting to mitigate the actual and future
10 consequences of the Data Breach, including but not limited to efforts spent researching how to
11 prevent, detect, contest, and recover from tax fraud and identity theft; (vi) costs associated with
12 placing freezes on credit reports; (vii) the continued risk to their PII and PHI, which remain in
13 Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails
14 to undertake appropriate and adequate measures to protect the PII and PHI of Plaintiff and the
15 Nationwide Class; and (viii) future costs in terms of time, effort, and money that will be expended
16 to prevent, detect, contest, and repair the impact of the PII and PHI compromised as a result of the
17 Data Breach for the remainder of the lives of Plaintiff and the Nationwide Class.

18 142. As a direct and proximate result of Defendant's breaches of confidence, Plaintiff and
19 the Nationwide Class have suffered and will continue to suffer other forms of injury and/or harm,
20 including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and
21 non-economic losses.

22 **COUNT VI**

23 **Violation of the California Unfair Competition Law,**
24 **Cal. Bus. & Prof. Code § 17200, *et seq.* – Unlawful Business Practices**
25 **(On Behalf of Plaintiff and the California Class)**

26 143. Plaintiff and the California Class re-allege and incorporate by reference herein all
27 the allegations contained in paragraphs 1 through 69.
28

1 144. Defendant has violated Cal. Bus. and Prof. Code § 17200, *et seq.*, by engaging in
2 unlawful, unfair, or fraudulent business acts and practices and unfair, deceptive, untrue, or
3 misleading advertising that constitute acts of “unfair competition” as defined in Cal. Bus. Prof.
4 Code § 17200 with respect to the services provided to the California Class.

5 145. Defendant engaged in unlawful acts and practices with respect to the services by
6 establishing the sub-standard security practices and procedures described herein; by soliciting and
7 collecting the PII and PHI of Plaintiff and the California Class with knowledge that the information
8 would not be adequately protected; and by storing the PII and PHI of Plaintiff and the California
9 Class in an unsecure environment in violation of California’s data breach statute, Cal. Civ. Code §
10 1798.81.5, which requires Defendant to take reasonable methods of safeguarding the PII and PHI
11 of Plaintiff and the California Class.

12 146. As a direct and proximate result of Defendant’s unlawful practices and acts, Plaintiff
13 and the California Class were injured and lost money or property, including but not limited to the
14 price received by Defendant for the services, the loss of Plaintiff’s and the California Class’s legally
15 protected interest in the confidentiality and privacy of their PII and PHI, nominal damages, and
16 additional losses as described above.

17 147. Defendant knew or should have known that Defendant’s data security practices were
18 inadequate to safeguard the PII and PHI of Plaintiff and the California Class and that the risk of a
19 data breach or theft was highly likely, especially given Defendant’s inability to adhere to basic
20 encryption standards and data disposal methodologies. Defendant’s actions in engaging in the
21 above-named unlawful practices and acts were negligent, knowing, and willful, and/or wanton and
22 reckless with respect to the rights of members of the California Class.

23 148. Plaintiff and the California Class seek relief under Cal. Bus. & Prof. Code § 17200,
24 *et seq.*, including, but not limited to, restitution to Plaintiff and the California Class of money or
25 property that Defendant may have acquired by means of Defendant’s unlawful, and unfair business
26 practices, restitutionary disgorgement of all profits accruing to Defendant because of Defendant’s
27
28

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

3 **COUNT VII**

4 **Violation of California's Unfair Competition Law,**
5 **Cal. Bus. & Prof. Code § 17200, *et seq.* – Unfair Business Practices**
6 **(On Behalf of Plaintiff and the California Class)**

7 149. Plaintiff and the California Class re-allege and incorporate by reference herein all
8 the allegations contained in paragraphs 1 through 69.

9 150. Defendant engaged in unfair acts and practices with respect to the services by
10 establishing the sub-standard security practices and procedures described herein by soliciting and
11 collecting the PII and PHI of Plaintiff and the California Class with knowledge that the information
12 would not be adequately protected and by storing the PII and PHI Plaintiff and the California Class
13 in an unsecure electronic environment. These unfair acts and practices were immoral, unethical,
14 oppressive, unscrupulous, unconscionable, and/or substantially injurious to Plaintiff and the
15 California Class. They were likely to deceive the public into believing their PII and PHI was
16 securely stored when it was not. The harm these practices caused to Plaintiff and the California
17 Class outweighed their utility, if any.

18 151. Defendant engaged in unfair acts and practices with respect to the provision of
19 services by failing to take proper action following the Data Breach to enact adequate privacy and
20 security measures and protect the PII and PHI of Plaintiff and the California Class from further
21 unauthorized disclosure, release, data breaches, and theft. These unfair acts and practices were
22 immoral, unethical, oppressive, unscrupulous, unconscionable, and/or substantially injurious to
23 Plaintiff and the California Class. They were likely to deceive the public into believing their PII
24 and PHI were securely stored when they were not. The harm these practices caused to Plaintiff and
25 the California Class outweighed their utility, if any.

26 152. As a direct and proximate result of Defendant's acts of unfair practices, Plaintiff and
27 the California Class were injured and lost money or property, including but not limited to the price
28

1 received by Defendant for the services, the loss of Plaintiff and the California Class's legally
2 protected interest in the confidentiality and privacy of their PII and PHI, nominal damages, and
3 additional losses as described above.

4 153. Defendant knew or should have known that Defendant's data security practices were
5 inadequate to safeguard the PII and PHI of Plaintiff and the California Class and that the risk of a
6 data breach or theft was highly likely, including Defendant's failure to properly encrypt files
7 containing sensitive PII and PHI. Defendant's actions in engaging in the above-named unlawful
8 practices and acts were negligent, knowing, and willful, and/or wanton and reckless with respect to
9 the rights of Plaintiff and the California Class.

10 154. Plaintiff and the California Class seek relief under Cal. Bus. & Prof. Code § 17200,
11 *et seq.*, including, but not limited to, restitution to Plaintiff and the California Class of money or
12 property that the Defendant may have acquired by means of Defendant's unfair business practices,
13 restitutionary disgorgement of all profits accruing to Defendant because of Defendant's unfair
14 business practices, declaratory relief, attorneys' fees, and costs (pursuant to Cal. Code Civ. Proc. §
15 1021.5), and injunctive or other equitable relief.

16 **COUNT VIII**

17 **Violation of California's Consumer Privacy Act, Cal. Civ. Code. § 1798.150**
18 **(On behalf of Plaintiff and the California Class)**

19 155. Plaintiff and the California Class re-allege and incorporate by reference herein all
20 the allegations contained in paragraphs 1 through 69.

21 156. Defendant violated section 1798.150(a) of the California Consumer Privacy Act
22 ("CCPA") by failing to prevent Plaintiff's and the California Class's nonencrypted and nonredacted
23 PII and PHI from unauthorized access and exfiltration, theft, or disclosure as a result of Defendant's
24 violations of its duty to implement and maintain reasonable security procedures and practices
25 appropriate to the nature of the information to protect the PII and PHI of Plaintiff and the California
26 Class.

1 157. As a direct and proximate result of Defendant's acts, Plaintiff's, and the California
2 Class's PII and PHI was subjected to unauthorized access and exfiltration, theft, or disclosure
3 through Defendant's computer systems.

4 158. As a direct and proximate result of Defendant's acts, Plaintiff and the California
5 Class were injured and lost money or property, including but not limited to the loss of the California
6 Class's legally protected interest in the confidentiality and privacy of their PII and PHI, nominal
7 damages, and additional losses as described above.

8 159. Defendant knew or should have known that their computer systems and data security
9 practices were inadequate to safeguard the California Class's PII and PHI and that the risk of a data
10 breach or theft was highly likely. Defendant failed to implement and maintain reasonable security
11 procedures and practices appropriate to the nature of the information to protect the personal
12 information of Plaintiff and the California Class.

13 160. Defendant is organized or operated for the profit or financial benefit of its
14 shareholders. Defendant collected Plaintiff's and Class Members PII and PHI as defined in Cal.
15 Civ. Code § 1798.140.

16 161. Defendant (a) has a gross annual revenue of over \$25 million and (b) buys, receives,
17 or sells the personal information of 50,000 or more California residents, households, or devices.

18 162. At this time, Plaintiff and the California Class seek only actual pecuniary damages
19 suffered as a result of Defendant's violations of the CCPA, injunctive and declaratory relief,
20 attorneys' fees, and costs (pursuant to Cal. Code Civ. Proc. § 1021.5), and any other relief the court
21 deems proper.

22 163. On May 10, 2021, Plaintiff separately provided written notice to Defendant
23 identifying the specific provisions of this title he alleges it has violated. On May 26, 2021,
24 Defendant responded that "[a]fter becoming aware of the data security incident, FPI promptly took
25 several steps to terminate any unauthorized access and prevent reoccurrence. This included, but
26 was not limited to, a forced password reset on all user accounts and user password audit to ensure
27 only authorized users have access. Endpoint monitoring and protected was added. Firewall border
28

1 security was enhanced. Additional steps were also taken to enhance security and prevent
2 unauthorized access.”

3 164. Defendant failed to actually cure its violations of Cal. Civ. Code
4 § 1798.150(a) because, among other things, it did not encrypt the PII and PHI of Plaintiff and the
5 California Class that it continued to maintain in an Internet-accessible environment and did not
6 delete the data of Plaintiff and the California Class that it no longer had a reasonable need to
7 maintain in an Internet-accessible environment. Accordingly, Plaintiff seeks statutory damages in
8 an amount not less than one hundred dollars (\$100) and not greater than seven hundred and fifty
9 (\$750) per consumer per incident or actual damages, whichever is greater. See Cal. Civ. Code §
10 1798.150(b).

11 **COUNT VIII**

12 **Violation Of The California Customer Records Act, § 1798, *et seq.*** 13 **(On behalf of Plaintiff and the California Class)**

14 165. Plaintiff and the California Class re-allege and incorporate by reference herein all
15 the allegations contained in paragraphs 1 through 69.

16 166. The Data Breach described above constituted a “breach of the security system” of
17 Defendant, within the meaning of Section 1798.82 (g) of the California Civil Code.

18 167. The information lost in the Data Breach constituted “personal information” within
19 the meaning of Section 1798.80(e) of the California Civil Code.

20 168. Under Cal Civ. Code § 1798.81.5(d)(1)(A)(i-iv), “personal information,” as
21 described in Cal Civ. Code § 1798.81.5(b), means the following:

22 (A) [a]n individual’s first name or first initial and his or her last name in
23 combination with any one or more of the following data elements, when either
24 the name or the data elements are not encrypted or redacted: (i) Social security
25 number. (ii) Driver’s license number or California identification card number.
26 (iii) Account number, credit or debit card number, in combination with any
27 required security code, access code, or password that would permit access to an
28 individual’s financial account.

1 169. Defendant failed to implement and maintain reasonable security procedures and
2 practices appropriate to the nature and scope of the information compromised in the Data Breach.

3 170. Defendant unreasonably delayed informing anyone about the breach of security of
4 Plaintiff and the Class Members' confidential and non-public information after Defendant knew
5 the Data Breach had occurred.

6 171. Defendant failed to disclose to Plaintiff and Class Members, without unreasonable
7 delay, and in the most expedient time possible, the breach of security of their unencrypted, or not
8 properly and securely encrypted, PII and PHI when they knew or reasonably believed such
9 information had been compromised.

10 172. By failing to promptly notify all affected members that their personal information
11 had been acquired (or was reasonably believed to have been acquired) by unauthorized persons in
12 the data breach, Defendant violated Civil Code section 1798.82 of the same title. Defendant's
13 failure to timely notify employees of the breach has caused class members damages who have had
14 to buy identity protection services or take other measures to remediate the breach caused by
15 Defendant's negligence.

16 173. Upon information and belief, no law enforcement agency instructed Defendant
17 that notification to Plaintiff and Class Members would impede investigation.

18 174. As a result of Defendant's violation of Cal. Civ. Code § 1798.80 *et seq.*, Plaintiff
19 and Class Members incurred economic damages, including expenses associated with necessary
20 credit monitoring.

21 175. Plaintiff, individually and on behalf of the Class, seeks all remedies available under
22 Cal. Civ. Code § 1798.84, including but not limited to: (a) damages suffered by the California
23 Subclass as alleged above; (b) statutory damages for Defendant's willful, intentional, and/or
24 reckless violation of Cal. Civ. Code § 1798.83; and (c) equitable relief. Additionally, as a result of
25 Defendant's violation of Civil Code sections 1798.81.5, and 1798.82, Plaintiff and Class Members
26 have and will incur economic damages relating to time and money spent remedying the breach,
27 including but not limited to, expenses for bank fees associated with the breach, any unauthorized
28

1 charges made on financial accounts, lack of access to funds while banks issue new cards, tax fraud,
2 as well as the costs of credit monitoring and purchasing credit reports.

3 176. Plaintiff, individually and on behalf of the Class, also seeks reasonable attorneys'
4 fees and costs under Cal. Civ. Code § 1798.84(g).

5 177. Because Defendant violated Cal. Civ. Code Sections 1798.81.5 and 1798.82, and
6 continues to violate Cal. Civ. Code Section 1798.82, Plaintiff may seek an injunction pursuant to
7 Cal. Civ. Code Section 1798.84(e), which states "[a]ny business that violates, proposes to violate,
8 or has violated this title may be enjoined." Specifically, Plaintiff seeks injunctive relief as follows
9 -- Defendant must implement and maintain adequate and reasonable data security measures and
10 abide by the California Data Breach laws, including, but not limited to:

- 11 a. hiring third-party security auditors and penetration testers in addition to internal
12 security personnel to conduct testing, including simulated attacks, penetration
13 tests, and audits on Defendant's systems periodically, and ordering Defendant to
14 promptly rectify any flaws or issues detected by such parties;
- 15 b. as required by Cal. Civ. Code Section 1798.81.5, "implement and maintain
16 reasonable security procedures and practices appropriate to the nature of the
17 information, to protect the personal information from unauthorized access,
18 destruction, use, modification, or disclosure;"
- 19 c. engaging third-party security auditors and internal personnel to run automated
20 security monitoring;
- 21 d. testing, auditing, and training their security personnel regarding any and all new
22 and/or modified security measures or procedures;
- 23 e. creating further and separate protections for customer data including, but not
24 limited to, the creation of firewalls and access controls so that if one area of
25 Defendant's data security measures are compromised, hackers cannot gain access
26 to other areas of Defendant's systems;

- f. deleting, in a reasonable and secure manner, Personal Information not necessary for Defendant's provisions of services;
- g. conducting regular database scanning and security checks;
- h. issue security breach notifications to California Residents which abide by the requirements established under Cal. Civ. Code Section 1798.82(d);
- i. conducting routine and periodic training and education to prepare internal security personnel regarding the processes to identify and contain a breach when it occurs and what appropriate actions are proper in response to a breach; and
- j. educating their customers about the threats they face as a result of the loss of their financial and personal information to third parties, as well as the steps customers must take to protect themselves and assisting with said steps by providing credit monitoring services.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of himself and Class Members, requests judgment against Defendant and that the Court grant the following:

- A. For an Order certifying the Nationwide Class and the California Class, and appointing Plaintiff and their Counsel to represent each such Class;
- B. For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of the PII and PHI of Plaintiff and Class Members, and from refusing to issue prompt, complete, any accurate disclosures to Plaintiff and Class Members;
- C. For injunctive relief requested by Plaintiff, including but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Plaintiff and Class Members, including but not limited to an order:
 - i. prohibiting Defendant from engaging in the wrongful and unlawful acts described herein;

- 1 ii. requiring Defendant to protect, including through encryption, all data collected
- 2 through the course of its business in accordance with all applicable regulations,
- 3 industry standards, and federal, state, or local laws;
- 4 iii. requiring Defendant to delete, destroy, and purge the personal identifying
- 5 information of Plaintiff and Class Members unless Defendant can provide to the
- 6 Court reasonable justification for the retention and use of such information when
- 7 weighed against the privacy interests of Plaintiff and Class Members;
- 8 iv. requiring Defendant to implement and maintain a comprehensive Information
- 9 Security Program designed to protect the confidentiality and integrity of the PII
- 10 and PHI of Plaintiff and Class Members;
- 11 v. prohibiting Defendant from maintaining the PII and PHI of Plaintiff and Class
- 12 Members on a cloud-based database;
- 13 vi. requiring Defendant to engage independent third-party security
- 14 auditors/penetration testers as well as internal security personnel to conduct
- 15 testing, including simulated attacks, penetration tests, and audits on Defendant's
- 16 systems on a periodic basis, and ordering Defendant to promptly correct any
- 17 problems or issues detected by such third-party security auditors;
- 18 vii. requiring Defendant to engage independent third-party security auditors and
- 19 internal personnel to run automated security monitoring;
- 20 viii. requiring Defendant to audit, test, and train its security personnel regarding any
- 21 new or modified procedures;
- 22 ix. requiring Defendant to segment data by, among other things, creating firewalls
- 23 and access controls so that if one area of Defendant's network is compromised,
- 24 hackers cannot gain access to other portions of Defendant's systems;
- 25 x. requiring Defendant to conduct regular database scanning and securing checks;
- 26 xi. requiring Defendant to establish an information security training program that
- 27 includes at least annual information security training for all employees, with
- 28

1 additional training to be provided as appropriate based upon the employees'
2 respective responsibilities with handling personal identifying information, as
3 well as protecting the personal identifying information of Plaintiff and Class
4 Members;

5 xii. requiring Defendant to routinely and continually conduct internal training and
6 education, and on an annual basis to inform internal security personnel how to
7 identify and contain a breach when it occurs and what to do in response to a
8 breach;

9 xiii. requiring Defendant to implement a system of tests to assess its respective
10 employees' knowledge of the education programs discussed in the preceding
11 subparagraphs, as well as randomly and periodically testing employee's
12 compliance with Defendant's policies, programs, and systems for protecting
13 personal identifying information;

14 xiv. requiring Defendant to implement, maintain, regularly review, and revise as
15 necessary a threat management program designed to appropriately monitor
16 Defendant's information networks for threats, both internal and external, and
17 assess whether monitoring tools are appropriately configured, tested, and
18 updated;

19 xv. requiring Defendant to meaningfully educate all Class Members about the
20 threats that they face as a result of the loss of their confidential personal
21 identifying information to third parties, as well as the steps affected individuals
22 must take to protect themselves;

23 xvi. requiring Defendant to implement logging and monitoring programs sufficient
24 to track traffic to and from Defendant's servers; and for a period of 10 years,
25 appointing a qualified and independent third-party assessor to conduct a SOC 2
26 Type 2 attestation on an annual basis to evaluate Defendant's compliance with
27 the terms of the Court's final judgment, to provide such report to the Court and
28

1 to counsel for the class, and to report any deficiencies with compliance of the
2 Court's final judgment;

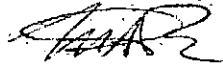
- 3 D. For an award of damages, including actual, nominal, statutory, and consequential
4 damages, as allowed by law in an amount to be determined;
- 5 E. For an award of attorneys' fees, costs, and litigation expenses, as allowed by law;
- 6 F. For prejudgment interest on all amounts awarded; and
- 7 G. Such other and further relief as this Court may deem just and proper.

8 **DEMAND FOR JURY TRIAL**

9 Plaintiff hereby demands that this matter be tried before a jury.

10
11 Date: September 26, 2022

**CLAYEO C. ARNOLD,
A PROFESSIONAL LAW CORP.**

12
13 

14 By: _____

M. Anderson Berry, Esq.
**CLAYEO C. ARNOLD,
A PROFESSIONAL LAW CORP.**

15
16 Michael F. Ram, Esq.
17 John A. Yanchunis, Esq.
18 Ryan D. Maxey, Esq.
**MORGAN & MORGAN
COMPLEX LITIGATION GROUP**

19
20 Kevin S. Hannon, Esq.
THE HANNON LAW FIRM, LLC

21 *Attorneys for Plaintiff and the Putative Class*
22
23
24
25
26
27
28

PROOF OF SERVICE

I, Lori Martin, declare and state:

I am a citizen of the United States, over 18 years of age, employed in the county of Sacramento, and not a party to the within action. My business address is 865 Howe Avenue, Sacramento, CA 95825.

On the date set forth below, I served the following on the parties in said action by the means indicated below:

FIRST AMENDED CLASS ACTION COMPLAINT

☐ (BY MAIL) I caused such envelope with postage thereon fully prepaid to be placed in the United States mail at Sacramento, California. I am familiar with my firm's practice whereby the mail is given the appropriate postage and is placed in the designated area to be deposited in a U.S. mail box in Sacramento, California, in the ordinary course of business;

☐ (BY EXPRESS MAIL) I caused such envelope to be placed in the U.S. Mail/UPS depository at Sacramento, California; overnight service;

☐ (BY PERSONAL SERVICE) delivered by hand to addressee at the address listed below;

☐ (BY FACSIMILE/TELECOPIER) I personally sent to the addressee's telecopier number (stated below) a true copy of the above-described documents.

☒ (BY TRANSMITTING VIA EMAIL OR ELECTRONIC TRANSMISSION) the document(s) listed above to the addressees listed below at the email addresses indicated, from lori@justice4you.com:

Michael F. Ram, Esq. (SBN 104805)
MORGAN & MORGAN
COMPLEX LITIGATION GROUP
711 Van Ness Avenue, Suite 500
San Francisco, CA 94102
Telephone: (415) 358-6913
Facsimile: (415) 358-6923
Email: mram@forthepeople.com

John A. Yanchunis, Esq. (*Pro Hac Vice*)
Ryan D. Maxey, Esq. (*Pro Hac Vice*)
MORGAN & MORGAN
COMPLEX LITIGATION GROUP
201 N. Franklin Street, 7th Floor
Tampa, Florida 33602
Telephone: (813) 223-5505
Email: jyanchunis@ForThePeople.com;
rmaxey@ForThePeople.com

Jon P. Kardassakis, Esq. SBN 90602
LEWIS BRISBOIS BISGAARD & SMITH LLP
633 West 5th Street, Suite 4000
Los Angeles, California 90071
Telephone: (213) 250-1800
Facsimile: (213) 250-7900
Email: Jon.Kardassakis@lewisbrisbois.com

Joann M. O. Rangel, Esq. SBN 200228
LEWIS BRISBOIS BISGAARD & SMITH LLP
2020 West El Camino Avenue, Suite 700
Sacramento, California 95833
Telephone: (916) 564-5400
Facsimile: (916) 564-5444
Email: Joann.Rangel@lewisbrisbois.com

Attorneys for Defendant,
FPI MANAGEMENT, INC.

Kevin S. Hannon, Esq.
THE HANNON LAW FIRM, LLC
1641 North Downing Street
Denver, Colorado 80218
Telephone: (303) 861-8800
Email: khannon@hannonlaw.com

Co-Counsel for Plaintiff and the Proposed Class

I declare under penalty of perjury under the laws of the state of California that the foregoing is true and correct. Executed on September 27, 2022, at Sacramento, California.

/s/ Lori Martin

Lori Martin