

FILED/ENDORSED

MAY 12 2022

By: M. Valledor
Deputy Clerk

MICHAEL F. RAM (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
mram@forthepeople.com

M. ANDERSON BERRY (SBN 262879)
GREGORY HAROUTUNIAN (SBN 330263)
CLAYEO C. ARNOLD,
A PROFESSIONAL LAW CORP.
865 Howe Avenue
Sacramento, CA 95825
Telephone: (916) 239-4778
Facsimile: (916) 924-1829
aberry@justice4you.com
gharoutunian@justice4you.com

JOHN A. YANCHUNIS
(Pro Hac Vice application pending)
RYAN D. MAXEY
(Pro Hac Vice application pending)
MORGAN & MORGAN COMPLEX
LITIGATION GROUP
201 N. Franklin Street, 7th Floor
Tampa, Florida 33602
(813) 223-5505
jyanchunis@ForThePeople.com
rmaxey@ForThePeople.com

KEVIN S. HANNON
THE HANNON LAW FIRM, LLC
1641 North Downing Street
Denver, Colorado 80218
303-861-8800
khannon@hannonlaw.com

Attorneys for Plaintiff and the Putative Class

SUPERIOR COURT OF THE STATE OF CALIFORNIA

COUNTY OF SACRAMENTO

BY FAX

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

4 Plaintiff,

5 vs.

6 FPI MANAGEMENT, INC.,

7 Defendant.

Case No.: 34-2021-00300923

MOTION TO AMEND COMPLAINT

Date: July 15, 2022

Time: 9:00 a.m.

Dept.: 25

Judge: Jill H. Talley

Reservation #: 2645103

8 Plaintiff, Richard Archibeque, pursuant to California Rules of Court 3.1324, moves to
9 amend the complaint and states as follows:

10 1. Plaintiff seeks to amend the complaint filed in this matter to demand statutory
11 damages under the California Consumer Privacy Act (the "CCPA"), § 1798.100 et al. A copy of
12 the proposed amended complaint is attached as Exhibit A.

13 2. Plaintiff filed the original complaint on May 17, 2021, which Defendant Answered
14 on July 12, 2021.

15 3. The CCPA requires a consumer, before seeking statutory damages under the CCPA,
16 to afford the defendant an opportunity to cure, as follows:

17 Actions pursuant to this section may be brought by a consumer if, prior
18 to initiating any action against a business for statutory damages on an
19 individual or class-wide basis, a consumer provides a business 30 days'
20 written notice identifying the specific provisions of this title the
21 consumer alleges have been or are being violated. In the event a cure is
22 possible, if within the 30 days the business actually cures the noticed
23 violation and provides the consumer an express written statement that
24 the violations have been cured and that no further violations shall occur,
25 no action for individual statutory damages or class-wide statutory
26 damages may be initiated against the business.
27
28

1 § 1798.150(b).

2 4. On or around May 10, 2021, Plaintiff sent Defendant written notice that it had failed
3 to prevent Plaintiffs' and other California residents' nonencrypted and nonredacted personally
4 identifiable information ("PII"), including Social Security numbers, from unauthorized accessed
5 and exfiltration, theft, or disclosure. Plaintiff further demanded that FPI cure the violation of the
6 CCPA which exposed the nonencrypted and nonredacted PII.

7 5. On or around May 26, 2021, Defendant sent Plaintiff a written response stating that
8 it had done the following:

9
10 After becoming aware of the data security incident, FPI promptly took
11 several steps to terminate any unauthorized access and prevent
12 reoccurrence. This included, but was not limited to, a forced password
13 reset on all user accounts and user password audit to ensure only
14 authorized users have access. Endpoint monitoring and access was
15 added. Firewall border security was enhanced. Additional steps were
16 also taken to enhance security and prevent unauthorized access.
17

18 6. In its written response, Defendant did not claim to have encrypted or redacted the
19 sensitive PII, including Social Security numbers, of Plaintiff and others similarly situated.
20 Defendant also did not claim to have removed the sensitive PII, including Social Security numbers,
21 of Plaintiff and others similarly situated from the Internet-accessible environment where the
22 security incident occurred. Finally, Defendant did not claim to have deleted the sensitive PII,
23 including Social Security numbers, of Plaintiffs and others similarly situated that Defendant did
24 not have a reasonable need to maintain.

25 7. By failing to take the above actions, Defendant necessarily failed to actually cure
26 its violations of the CCPA. Accordingly, Plaintiff seeks to amend the complaint to seek statutory
27 damages under the CCPA.
28

1 8. The proposed amended complaint modifies paragraphs 163 and 164 on page 30 to
2 remove language stating that Plaintiff would amend the complaint to seek statutory damages if
3 Defendant failed to cure its violations of the CCPA within 30 days of receiving Plaintiff's written
4 notice and replacing such language as follows:

5 163. On May 26, 2021, Defendant responded that "[a]fter becoming
6 aware of the data security incident, FPI promptly took several steps to
7 terminate any unauthorized access and prevent reoccurrence. This
8 included, but was not limited to, a forced password reset on all user
9 accounts and user password audit to ensure only authorized users have
10 access. Endpoint monitoring and protected was added. Firewall border
11 security was enhanced. Additional steps were also taken to enhance
12 security and prevent unauthorized access."

13
14 164. Defendant failed to actually cure its violations of Cal. Civ. Code
15 § 1798.150(a) because, among other things, it did not encrypt the PII
16 and PHI of Plaintiff and the California Class that it continued to
17 maintain in an Internet-accessible environment and did not delete the
18 data of Plaintiff and the California Class that it no longer had a
19 reasonable need to maintain in an Internet-accessible environment.
20 Accordingly, Plaintiff seeks statutory damages in an amount not less
21 than one hundred dollars (\$100) and not greater than seven hundred and
22 fifty (\$750) per consumer per incident or actual damages, whichever is
23 greater. See Cal. Civ. Code § 1798.150(b).

24 9. The proposed amended complaint modifies subsection "D" of the prayer for relief
25 on page 36 to include statutory damages among the others forms of damages for which Plaintiff
26 seeks an award.

27 10. The proposed amended complaint includes the word "Amended" as appropriate to
28 make clear it is an amended complaint.

1 11. Plaintiff's counsel, John A. Yanchunis, declares that (i) the effect of the amendment
2 is to allow Plaintiff, on behalf of himself and others similarly situated, to seek statutory damages
3 under the CCPA, (ii) the amendment is necessary and proper to allow Plaintiff to seek such
4 damages, (iii) the facts giving rise to the amended allegations were discovered when Plaintiff
5 received Defendant's written response to Plaintiff's written notice, and (iv) the amendment was
6 not made earlier because at the time Plaintiff filed the complaint Plaintiff had not yet received
7 Defendant's written response to Plaintiff's written notice. See Exhibit B (Declaration of John A.
8 Yanchunis) ¶¶ 4-7.

9 WHEREFORE, Plaintiff respectfully requests that the Court enter an order granting
10 Plaintiff leave to file the proposed amended complaint.

11
12
13 Date: May 9, 2022

Respectfully Submitted,

14 By: /s/ M. Anderson Berry
15 M. Anderson Berry

16 M. ANDERSON BERRY (SBN 262879)
17 GREGORY HAROUTUNIAN (SBN 330263)
18 **CLAYEO C. ARNOLD,**
19 **A PROFESSIONAL LAW CORP.**
20 865 Howe Avenue
21 Sacramento, CA 95825
22 Telephone: (916) 239-4778
23 Facsimile: (916) 924-1829
24 aberry@justice4you.com
25 gharoutunian@justice4you.com

26 MICHAEL F. RAM (SBN 104805)
27 **MORGAN & MORGAN**
28 **COMPLEX LITIGATION GROUP**
29 711 Van Ness Avenue, Suite 500
30 San Francisco, CA 94102
31 Telephone: (415) 358-6913
32 Facsimile: (415) 358-6923
33 mram@forthepeople.com

34 JOHN A. YANCHUNIS
35 (Pro Hac Vice Pending)

1 RYAN D. MAXEY
2 (Pro Hac Vice Pending)
3 **MORGAN & MORGAN COMPLEX**
4 **LITIGATION GROUP**
5 201 N. Franklin Street, 7th Floor
6 Tampa, Florida 33602
7 (813) 223-5505
8 jyanchunis@ForThePeople.com
9 rmaxey@ForThePeople.com

10 KEVIN S. HANNON
11 **THE HANNON LAW FIRM, LLC**
12 1641 North Downing Street
13 Denver, Colorado 80218
14 303-861-8800
15 khannon@hannonlaw.com

16 *Attorneys for Plaintiff and the Putative Class*
17
18
19
20
21
22
23
24
25
26
27
28

Exhibit A

1 MICHAEL F. RAM (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 mram@forthepeople.com

9 M. ANDERSON BERRY (SBN 262879)
10 GREGORY HAROUTUNIAN (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 aberry@justice4you.com
18 gharoutunian@justice4you.com

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

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

Attorneys for Plaintiff and the Putative Class

SUPERIOR COURT OF THE STATE OF CALIFORNIA

COUNTY OF SACRAMENTO

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

4 Plaintiff,

5 vs.

6 FPI MANAGEMENT, INC.,

7 Defendant.

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

**AMENDED CLASS ACTION COMPLAINT
DEMAND FOR JURY TRIAL**

8
9 Plaintiff Richard Archibeque ("Plaintiff"), individually and on behalf of all others similarly
10 situated ("Class Members"), brings this Amended Class Action Complaint against FPI
11 Management, Inc. ("Defendant" or "FPI"), and alleges, upon personal knowledge as to his own
12 actions and his counsels' investigations, and upon information and belief as to all other matters, as
13 follows:

14 **I. INTRODUCTION**

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

22 2. According to Defendant's website, it "is a privately owned, exclusive third-party,
23 multifamily property manager."² Its "client list includes institutional investors, international real
24

25 ¹ Personally identifiable information generally incorporates information that can be used to distinguish or trace an
26 individual's identity, either alone or when combined with other personal or identifying information. 2 CFR § 200.79.
27 At a minimum, it includes all information that on its face expressly identifies an individual. PII also is generally
28 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).

² See <https://fpimgt.com/> (last visited May 9, 2022).

1 estate investment firms, financial institutions, multifamily development builders, private investors,
2 City, County, and State agencies.”³

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

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

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

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

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

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

24 9. Plaintiff brings this action on behalf of all persons whose PII and PHI was
25 compromised as a result of Defendant’s failure to: (i) adequately protect the PII and PHI of Plaintiff
26 and Class Members; (ii) warn Plaintiff and Class Members of its inadequate information security
27 practices; and (iii) avoid sharing the PII and PHI of Plaintiff and Class Members without adequate

28 ³ *Id.*

1 safeguards. Defendant's conduct amounts to negligence and violates federal and state statutes.

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

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

20 II. PARTIES

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

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

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

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

3 **III. JURISDICTION AND VENUE**

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

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

10 **IV. FACTUAL ALLEGATIONS**

11 ***Background***

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

19 19. Plaintiff and Class Members relied on this sophisticated Defendant to keep their PII
20 and PHI confidential and securely maintained, to use this information for business purposes only,
21 and to make only authorized disclosures of this information. Plaintiff and Class Members demand
22 security to safeguard their PII and PHI.

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

25 ***The Data Breach***

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

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

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

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

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

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

26 23. In response to the Data Breach, Defendant claims that it "immediately began
27
28

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

1 containment, mitigation, and restoration efforts” and “implemented additional security measures
2 to further harden its digital environment in an effort to prevent a similar event from occurring in
3 the future.”⁵ However, the details of the root cause of the Data Breach, the vulnerabilities
4 exploited, and the remedial measures undertaken to ensure a breach does not occur again have not
5 been shared with regulators or Plaintiff and Class Members, who retain a vested interest in ensuring
6 that their information remains protected.

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

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

14 ***Defendant Acquires, Collects and Stores Plaintiff’s and Class Members’ PII and PHI.***

15 26. Defendant acquired, collected, and stored Plaintiff’s and Class Members’ PII and
16 PHI.

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

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

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

26 ***Securing PII and PHI and Preventing Breaches***

27 30. Defendant could have prevented this Data Breach by properly securing and
28

⁵ *Id.*

1 encrypting the PII and PHI of Plaintiff and Class Members. Alternatively, Defendant could have
2 destroyed the data, especially decade-old data from former residents.

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

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

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

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

20 ***Value of Personal Identifiable Information***

21 35. The PII of individuals remains of high value to criminals, as evidenced by the prices
22 they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity
23 credentials. For example, personal information can be sold at a price ranging from \$40 to \$200,
24 and bank details have a price range of \$50 to \$200.⁸ Experian reports that a stolen credit or debit

25
26 ⁶ 17 C.F.R. § 248.201 (2013).

27 ⁷ *Id.*

28 ⁸ *Your personal data is for sale on the dark web. Here's how much it costs*, Digital Trends, Oct. 16, 2019, available at: <https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/> (last accessed May 9, 2022).

1 card number can sell for \$5 to \$110 on the dark web.⁹ Criminals can also purchase access to entire
2 company data breaches from \$900 to \$4,500.¹⁰

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

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

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

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

26 ⁹ *Here's How Much Your Personal Information Is Selling for on the Dark Web*, Experian, Dec. 6, 2017, available at:
27 <https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/> (last accessed May 9, 2022).

28 ¹⁰ *In the Dark*, VPNOOverview, 2019, available at: <https://vpnooverview.com/privacy/anonymous-browsing/in-the-dark/> (last accessed May 9, 2022).

¹¹ Social Security Administration, *Identity Theft and Your Social Security Number*, available at:
<https://www.ssa.gov/pubs/EN-05-10064.pdf> (last accessed May 9, 2022).

¹² Bryan Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR (Feb. 9, 2015),
available at: <http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millionsworrying-about-identity-theft> (last accessed May 9, 2022).

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

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

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

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

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

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

24 44. At all relevant times, Defendant knew, or reasonably should have known, of the
25 importance of safeguarding the PII and PHI of Plaintiff and Class Members, including Social
26 Security numbers and/or dates of birth, and of the foreseeable consequences that would occur if
the PII and PHI was compromised, including, specifically, the significant costs that would be

27 ¹³ Time Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, IT World,
(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 May 9, 2022).

28 ¹⁴ *Report to Congressional Requesters*, GAO, at 29 (June 2007), available at: <https://www.gao.gov/products/gao-07-737> (last accessed May 9, 2022).

1 imposed on Plaintiff and Class Members a result.

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

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

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

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

17 ***Plaintiff Richard Archibeque's Experience***

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

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

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

27 52. Additionally, Plaintiff Archibeque is very careful about sharing his PII and PHI.

28

¹⁵ Ex. 2.

1 He has never knowingly transmitted unencrypted PII or PHI over the internet or any other
2 unsecured source.

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

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

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

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

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

19 V. CLASS ALLEGATIONS

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

23 59. The Nationwide Class that Plaintiff seeks to represent is defined as follows:
24 All individuals residing in the United States whose PII or PHI was
25 accessed or acquired without authorization during the data breach
26 referenced in the Notice of Data Breach that Defendant sent to Plaintiff
on or around April 14, 2021 (the "Nationwide Class").

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

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

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

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

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

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

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

- 27 a. Whether and to what extent Defendant had a duty to protect the PII and PHI of Plaintiff
28 and Class Members;
- b. Whether Defendant had a duty not to disclose the PII and PHI of Plaintiff and Class

- 1 Members to unauthorized third parties;
- 2 c. Whether Defendant had a duty not to use the PII and PHI of Plaintiff and Class
- 3 Members for non-business purposes;
- 4 d. Whether Defendant failed to adequately safeguard the PII and PHI of Plaintiff and
- 5 Class Members;
- 6 e. Whether and when Defendant actually learned of the Data Breach;
- 7 f. Whether Defendant adequately, promptly, and accurately informed Plaintiff and Class
- 8 Members that their PII and PHI had been compromised;
- 9 g. Whether Defendant violated the law by failing to promptly notify Plaintiff and Class
- 10 Members that their PII and PHI had been compromised;
- 11 h. Whether Defendant failed to implement and maintain reasonable security procedures
- 12 and practices appropriate to the nature and scope of the information compromised in
- 13 the Data Breach;
- 14 i. Whether Defendant adequately addressed and fixed the vulnerabilities which permitted
- 15 the Data Breach to occur;
- 16 j. Whether Defendant engaged in unfair, unlawful, or deceptive practices by failing to
- 17 safeguard the PII and PHI of Plaintiff and Class Members;
- 18 k. Whether Plaintiff and Class Members are entitled to actual, damages, and/or statutory
- 19 damages as a result of Defendant's wrongful conduct;
- 20 l. Whether Plaintiff and Class Members are entitled to restitution as a result of
- 21 Defendant's wrongful conduct; and
- 22 m. Whether Plaintiff and Class Members are entitled to injunctive relief to redress the
- 23 imminent and currently ongoing harm faced as a result of the Data Breach.
- 24 66. Plaintiff is a member of the Classes he seeks to represent and his claims and injuries
- 25 are typical of the claims and injuries of the other Class Members.
- 26 67. Plaintiff will adequately and fairly protect the interests of other Class Members.
- 27 Plaintiff has no interests adverse to the interests of absent Class Members. Plaintiff is represented
- 28 by legal counsel with substantial experience in class action litigation. The interests of Class

1 Members will be fairly and adequately protected by Plaintiff and his counsel.

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

5 69. A class action is superior to other available means for fair and efficient adjudication
6 of the claims of the Class and would be beneficial for the parties and the court. Class action
7 treatment will allow a large number of similarly situated persons to prosecute their common claims
8 in a single forum, simultaneously, efficiently, and without the unnecessary duplication of effort
9 and expense that numerous individual actions would require. The amounts owed to the many
10 individual Class Members are likely to be relatively small, and the burden and expense of
11 individual litigation would make it difficult or impossible for individual members of the class to
12 seek and obtain relief. A class action will serve an important public interest by permitting such
13 individuals to effectively pursue recovery of the sums owed to them. Further, class litigation
14 prevents the potential for inconsistent or contradictory judgments raised by individual litigation.
15 Plaintiff is unaware of any difficulties that are likely to be encountered in the management of this
16 action that would preclude its maintenance as a class action.

17 **COUNT I**

18 **Negligence**

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

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

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

27 72. Plaintiff and the Nationwide Class entrusted their PII and PHI to Defendant on the
28 premise and with the understanding that Defendant would safeguard their information, use their

1 PII and PHI for business purposes only, and/or not disclose their PII and PHI to unauthorized third
2 parties.

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

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

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

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

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

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

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

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

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

6 82. Defendant's own conduct created a foreseeable risk of harm to Plaintiff and the
7 Nationwide Class. Defendant's misconduct included, but was not limited to, its failure to take the
8 steps and opportunities to prevent the Data Breach as set forth herein. Defendant's misconduct
9 also included its decisions not to comply with industry standards for the safekeeping of the PII and
10 PHI of Plaintiff and the Nationwide Class, including basic encryption techniques freely available
11 to Defendant.

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

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

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

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

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

26 88. Defendant, through its actions and/or omissions, unlawfully breached its duties to
27 Plaintiff and the Nationwide Class by failing to implement industry protocols and exercise
28 reasonable care in protecting and safeguarding the PII and PHI of Plaintiff and the Nationwide

1 Class during the time the PII and PHI was within Defendant's possession or control.

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

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

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

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

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

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

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

26 96. Additionally, Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting
27 commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by
28 businesses, such as Defendant, of failing to use reasonable measures to protect PII and PHI. The

1 FTC publications and orders described above also form part of the basis of Defendant's duty in
2 this regard.

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

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

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

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

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

1 lives of Plaintiff and the Nationwide Class.

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

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

11 **COUNT II**
12 **Breach of Written Contract**
13 **(On Behalf of Plaintiff and the Nationwide Class)**

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

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

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

22 **Information Security and Data Privacy Practice**

23 FPI Management follows the **NIST CyberSecurity Framework**
24 (National Institute of Standards and Technology) in setting our security
25 policies and security operations along with using encryption protocols
26 for data in transit and at rest in our systems. Although no information
27 transmitted across the internet can be guaranteed to be secure, we
28 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.

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 of the allegations contained in paragraphs 1 through 69.

¹⁶ Ex. 3 (emphasis in original).

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

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

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

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

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

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

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

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

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

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

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

COUNT V
Breach of Confidence
(On Behalf of Plaintiff and the Nationwide Class)

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

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

133. As alleged herein and above, Defendant's relationship with Plaintiff and the Nationwide Class was governed by terms and expectations that Plaintiff's and the Nationwide Class's PII and PHI would be collected, stored, and protected in confidence, and would not be disclosed to unauthorized third parties.

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

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

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

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

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

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

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

27 141. As a direct and proximate result of Defendant's breach of its confidence with
28 Plaintiff and the Nationwide Class, Plaintiff and the Nationwide Class have suffered and will suffer

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

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

18 **COUNT VI**

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

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

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

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

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

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

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

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

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

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

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

20 152. As a direct and proximate result of Defendant's acts of unfair practices, Plaintiff
21 and the California Class were injured and lost money or property, including but not limited to the
22 price received by Defendant for the services, the loss of Plaintiff and the California Class's legally
23 protected interest in the confidentiality and privacy of their PII and PHI, nominal damages, and
24 additional losses as described above.

25 153. Defendant knew or should have known that Defendant's data security practices
26 were inadequate to safeguard the PII and PHI of Plaintiff and the California Class and that the risk
27 of a data breach or theft was highly likely, including Defendant's failure to properly encrypt files
28 containing sensitive PII and PHI. Defendant's actions in engaging in the above-named unlawful

1 practices and acts were negligent, knowing and willful, and/or wanton and reckless with respect
2 to the rights of Plaintiff and the California Class.

3 154. Plaintiff and the California Class seek relief under Cal. Bus. & Prof. Code § 17200,
4 *et seq.*, including, but not limited to, restitution to Plaintiff and the California Class of money or
5 property that the Defendant may have acquired by means of Defendant's unfair business practices,
6 restitutionary disgorgement of all profits accruing to Defendant because of Defendant's unfair
7 business practices, declaratory relief, attorneys' fees and costs (pursuant to Cal. Code Civ. Proc. §
8 1021.5), and injunctive or other equitable relief.

9 **COUNT VIII**

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

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

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

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

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

27 159. Defendant knew or should have known that their computer systems and data
28 security practices were inadequate to safeguard the California Class's PII and PHI and that the risk

1 of a data breach or theft was highly likely. Defendant failed to implement and maintain reasonable
2 security procedures and practices appropriate to the nature of the information to protect the
3 personal information of Plaintiff and the California Class.

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

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

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

13 163. On May 10, 2021, Plaintiff separately provided written notice to Defendant
14 identifying the specific provisions of this title he alleges it has violated. On May 26, 2021,
15 Defendant responded that "[a]fter becoming aware of the data security incident, FPI promptly took
16 several steps to terminate any unauthorized access and prevent reoccurrence. This included, but
17 was not limited to, a forced password reset on all user accounts and user password audit to ensure
18 only authorized users have access. Endpoint monitoring and protected was added. Firewall border
19 security was enhanced. Additional steps were also taken to enhance security and prevent
20 unauthorized access."

21 164. Defendant failed to actually cure its violations of Cal. Civ. Code
22 § 1798.150(a) because, among other things, it did not encrypt the PII and PHI of Plaintiff and the
23 California Class that it continued to maintain in an Internet-accessible environment and did not
24 delete the data of Plaintiff and the California Class that it no longer had a reasonable need to
25 maintain in an Internet-accessible environment. Accordingly, Plaintiff seeks statutory damages in
26 an amount not less than one hundred dollars (\$100) and not greater than seven hundred and fifty
27 (\$750) per consumer per incident or actual damages, whichever is greater. See Cal. Civ. Code §
28 1798.150(b).

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

COUNT VIII

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

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

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

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

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

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

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

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

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

172. By failing to promptly notify all affected members that their personal information had been acquired (or was reasonably believed to have been acquired) by unauthorized persons in

1 the data breach, Defendant violated Civil Code section 1798.82 of the same title. Defendant's
2 failure to timely notify employees of the breach has caused class members damages who have had
3 to buy identity protection services or take other measures to remediate the breach caused by
4 Defendant's negligence.

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

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

10 175. Plaintiff, individually and on behalf of the Class, seeks all remedies available under
11 Cal. Civ. Code § 1798.84, including but not limited to: (a) damages suffered by the California
12 SubClass as alleged above; (b) statutory damages for Defendant's willful, intentional, and/or
13 reckless violation of Cal. Civ. Code § 1798.83; and (c) equitable relief. Additionally, as a result
14 of Defendant's violation of Civil Code sections 1798.81.5, and 1798.82, Plaintiff and Class
15 Members have and will incur economic damages relating to time and money spent remedying the
16 breach, including but not limited to, expenses for bank fees associated with the breach, any
17 unauthorized charges made on financial accounts, lack of access to funds while banks issue new
18 cards, tax fraud, as well as the costs of credit monitoring and purchasing credit reports.

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

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

- 27 a. hiring third-party security auditors and penetration testers in addition to internal
28 security personnel to conduct testing, including simulated attacks, penetration

1 tests, and audits on Defendant's systems periodically, and ordering Defendant to
2 promptly rectify any flaws or issues detected by such parties;

3 b. as required by Cal. Civ. Code Section 1798.81.5, "implement and maintain
4 reasonable security procedures and practices appropriate to the nature of the
5 information, to protect the personal information from unauthorized access,
6 destruction, use, modification, or disclosure;"

7 c. engaging third-party security auditors and internal personnel to run automated
8 security monitoring;

9 d. testing, auditing, and training their security personnel regarding any and all new
10 and/or modified security measures or procedures;

11 e. creating further and separate protections for customer data including, but not
12 limited to, the creation of firewalls and access controls so that if one area of
13 Defendant's data security measures are compromised, hackers cannot gain
14 access to other areas of Defendant's systems;

15 f. deleting, in a reasonable and secure manner, Personal Information not necessary
16 for Defendant's provisions of services;

17 g. conducting regular database scanning and security checks;

18 h. issue security breach notifications to California Residents which abide by the
19 requirements established under Cal. Civ. Code Section 1798.82(d);

20 i. conducting routine and periodic training and education to prepare internal
21 security personnel regarding the processes to identify and contain a breach when
22 it occurs and what appropriate actions are proper in response to a breach; and

23 j. educating their customers about the threats they face as a result of the loss of
24 their financial and personal information to third parties, as well as the steps
25 customers must take to protect themselves and assisting with said steps by
26 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;
 - ii. requiring Defendant to protect, including through encryption, all data collected through the course of its business in accordance with all applicable regulations, industry standards, and federal, state or local laws;
 - iii. requiring Defendant to delete, destroy, and purge the personal identifying information of Plaintiff and Class Members unless Defendant can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiff and Class Members;
 - iv. requiring Defendant to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of the PII and PHI of Plaintiff and Class Members;
 - v. prohibiting Defendant from maintaining the PII and PHI of Plaintiff and Class Members on a cloud-based database;
 - vi. requiring Defendant to engage independent third-party security auditors/penetration testers as well as internal security personnel to conduct

- 1 testing, including simulated attacks, penetration tests, and audits on
2 Defendant's systems on a periodic basis, and ordering Defendant to promptly
3 correct any problems or issues detected by such third-party security auditors;
- 4 vii. requiring Defendant to engage independent third-party security auditors and
5 internal personnel to run automated security monitoring;
- 6 viii. requiring Defendant to audit, test, and train its security personnel regarding any
7 new or modified procedures;
- 8 ix. requiring Defendant to segment data by, among other things, creating firewalls
9 and access controls so that if one area of Defendant's network is compromised,
10 hackers cannot gain access to other portions of Defendant's systems;
- 11 x. requiring Defendant to conduct regular database scanning and securing checks;
- 12 xi. requiring Defendant to establish an information security training program that
13 includes at least annual information security training for all employees, with
14 additional training to be provided as appropriate based upon the employees'
15 respective responsibilities with handling personal identifying information, as
16 well as protecting the personal identifying information of Plaintiff and Class
17 Members;
- 18 xii. requiring Defendant to routinely and continually conduct internal training and
19 education, and on an annual basis to inform internal security personnel how to
20 identify and contain a breach when it occurs and what to do in response to a
21 breach;
- 22 xiii. requiring Defendant to implement a system of tests to assess its respective
23 employees' knowledge of the education programs discussed in the preceding
24 subparagraphs, as well as randomly and periodically testing employees
25 compliance with Defendant's policies, programs, and systems for protecting
26 personal identifying information;
- 27 xiv. requiring Defendant to implement, maintain, regularly review, and revise as
28 necessary a threat management program designed to appropriately monitor

1 Defendant's information networks for threats, both internal and external, and
2 assess whether monitoring tools are appropriately configured, tested, and
3 updated;

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

8 xvi. requiring Defendant to implement logging and monitoring programs sufficient
9 to track traffic to and from Defendant's servers; and for a period of 10 years,
10 appointing a qualified and independent third party assessor to conduct a SOC 2
11 Type 2 attestation on an annual basis to evaluate Defendant's compliance with
12 the terms of the Court's final judgment, to provide such report to the Court and
13 to counsel for the class, and to report any deficiencies with compliance of the
14 Court's final judgment;

15 D. For an award of damages, including actual, nominal, statutory, and consequential
16 damages, as allowed by law in an amount to be determined;

17 E. For an award of attorneys' fees, costs, and litigation expenses, as allowed by law;

18 F. For prejudgment interest on all amounts awarded; and

19 G. Such other and further relief as this Court may deem just and proper.

20 **DEMAND FOR JURY TRIAL**

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

22 Date: May 9, 2022

Respectfully Submitted,

23 By: /s/ M. Anderson Berry
24 M. Anderson Berry

25 M. ANDERSON BERRY (SBN 262879)
26 GREGORY HAROUTUNIAN (SBN 330263)
27 CLAYEO C. ARNOLD,
A PROFESSIONAL LAW CORP.
865 Howe Avenue
Sacramento, CA 95825
Telephone: (916) 239-4778

Facsimile: (916) 924-1829
aberry@justice4you.com
gharoutunian@justice4you.com

MICHAEL F. RAM (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
mram@forthepeople.com

JOHN A. YANCHUNIS
(*Pro Hac Vice*)
RYAN D. MAXEY
(*Pro Hac Vice application forthcoming*)
MORGAN & MORGAN COMPLEX
LITIGATION GROUP
201 N. Franklin Street, 7th Floor
Tampa, Florida 33602
(813) 223-5505
jyanchunis@ForThePeople.com
rmaxey@ForThePeople.com

KEVIN S. HANNON
THE HANNON LAW FIRM, LLC
1641 North Downing Street
Denver, Colorado 80218
303-861-8800
khannon@hannonlaw.com

Attorneys for Plaintiff and the Putative Class

EXHIBIT 1

<<Date>> (Format: Month Day, Year)

<<first_name>> <<middle_name>> <<last_name>> <<suffix>>
<<address_1>>
<<address_2>>
<<city>>, <<state_province>> <<postal_code>>
<<country >>

Re: Notice of Data Breach

Dear <<first_name>> <<middle_name>> <<last_name>> <<suffix>>,

I am writing to inform you of a data security incident recently experienced by FPI Management ("FPI") that may have impacted your personal information. FPI takes the privacy and security of all information within its possession very seriously, which is why I am writing to notify you of this incident and to inform you of steps that can be taken to help safeguard your information.

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

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

What Information Was Involved: The incident may have impacted your 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, and / or medical information.

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

In connection with this incident, and out of an abundance of caution, FPI is offering complimentary identity theft protection services through Experian IdentityWorksSM. Enrollment instructions can be found on the next page of this letter.

What You Can Do: While we are not aware of any misuse of potentially impacted information in connection with the incident, as a precautionary measure, we recommend that you remain vigilant and review your account statements and credit reports closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company that maintains your account. You should also promptly report any fraudulent activity or any suspected incidents of identity theft to proper law enforcement authorities.

In addition, we encourage that you enroll in the complimentary one-year membership of Experian's® IdentityWorksSM credit monitoring and identity protection services we are offering. To activate your membership and start monitoring your personal information please follow the steps below:

1. ENROLL by: <<b2b_text_1(EnrollmentDeadline)>> (Your code will not work after this date.)
2. Visit the **Experian IdentityWorks** website to enroll: <https://www.experianidworks.com/3bcredit>
3. PROVIDE the **Activation Code**: <<Member ID>>

If you have questions about the IdentityWorks product, need assistance with identity restoration or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at 877.890.9332 and provide the engagement code <<b2b_text_2(EngagementNumber)>>. To activate credit monitoring you must be over the age of 18, and have established credit in the U.S., a Social Security number in your name, and a U.S. residential address associated with your credit file.

For More Information: Further information about how to help protect your personal information appears on the following page. If you have questions or need assistance, please call 1-855-935-6094 from 6:00 a.m. to 3:30 p.m. Pacific Time, Monday through Friday. We remain committed to protecting your personal information and apologize for any worry or inconvenience this may cause you.

The security of your information is a top priority for FPI, and we are committed to safeguarding your data and privacy.

Sincerely,



Blaine M. Reeve
Chief Information Officer
FPI Management

Steps You Can Take to Protect Your Information

Review Your Account Statements and Notify Law Enforcement of Suspicious Activity: As a precautionary measure, we recommend that you remain vigilant by reviewing your account statements and credit reports closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. You also should promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, your state attorney general, and/or the Federal Trade Commission (FTC).

Copy of Credit Report: You may obtain a free copy of your credit report from each of the three major credit reporting agencies once every 12 months by visiting <http://www.annualcreditreport.com/>, calling toll-free 877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You can print this form at <https://www.annualcreditreport.com/cra/requestformfinal.pdf>. You also can contact one of the following three national credit reporting agencies:

TransUnion	Experian	Equifax	Free Annual Report
P.O. Box 1000	P.O. Box 9532	P.O. Box 740241	P.O. Box 105281
Chester, PA 19016	Allen, TX 75013	Atlanta, GA 30374	Atlanta, GA 30348
1-800-916-8800	1-888-397-3742	1-800-525-6285	1-877-322-8228
www.transunion.com	www.experian.com	www.equifax.com	annualcreditreport.com

Fraud Alert: You may want to consider placing a fraud alert on your credit report. An initial fraud alert is free and will stay on your credit file for at least one year. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any accounts in your name. To place a fraud alert on your credit report, contact any of the three credit reporting agencies identified above. Additional information is available at <http://www.annualcreditreport.com>.

Security Freeze: Under U.S. law, you have the right to put a security freeze on your credit file for up to one year at no cost. This will prevent new credit from being opened in your name without the use of a PIN number that is issued to you when you initiate the freeze. A security freeze is designed to prevent potential creditors from accessing your credit report without your consent. As a result, using a security freeze may interfere with or delay your ability to obtain credit. You must separately place a security freeze on your credit file with each credit reporting agency. In order to place a security freeze, you may be required to provide the consumer reporting agency with information that identifies you including your full name, Social Security number, date of birth, current and previous addresses, a copy of your state-issued identification card, and a recent utility bill, bank statement or insurance statement.

Additional Free Resources: You can obtain information from the consumer reporting agencies, the FTC, or from your respective state attorney general about fraud alerts, security freezes, and steps you can take toward preventing identity theft. You may report suspected identity theft to local law enforcement, including to the FTC or to the attorney general in your state. Residents of Maryland, North Carolina, and Rhode Island can obtain more information from their attorneys general using the contact information below.

Federal Trade Commission	Maryland Attorney General	North Carolina Attorney General	Rhode Island Attorney General
600 Pennsylvania Ave, NW	200 St. Paul Place	9001 Mail Service Center	150 South Main Street
Washington, DC 20580	Baltimore, MD 21202	Raleigh, NC 27699	Providence, RI 02903
www.consumer.ftc.gov	www.oag.state.md.us	www.ncdoj.gov	www.riag.ri.gov
www.ftc.gov/idtheft	1-888-743-0023	1-877-566-7226	401-274-4400
1-877-438-4338			

You also have certain rights under the Fair Credit Reporting Act (FCRA): These rights include the right to know what is in your file; to dispute incomplete or inaccurate information; to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information. For more information about the FCRA, and your rights pursuant to the FCRA, please visit http://files.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf.

Personal Information of a Minor: You can request that each of the three national credit reporting agencies perform a manual search for a minor's Social Security number to determine if there is an associated credit report. Copies of identifying information for the minor and parent/guardian may be required, including birth or adoption certificate, Social Security card, and government issued identification card. If a credit report exists, you should request a copy of the report and immediately report any fraudulent accounts to the credit reporting agency. You can also report any misuse of minor's information to the FTC at <https://www.identitytheft.gov/>. For more information about Child Identity Theft and instructions for requesting a manual Social Security number search, visit the FTC website: <https://www.consumer.ftc.gov/articles/0040-child-identity-theft>.

ADDITIONAL DETAILS REGARDING YOUR 12-MONTH EXPERIAN IDENTITYWORKS MEMBERSHIP:

A credit card is **not** required for enrollment in Experian IdentityWorks.

You can contact Experian **immediately** regarding any fraud issues, and have access to the following features once you enroll in Experian IdentityWorks:

- **Experian credit report at signup:** See what information is associated with your credit file. Daily credit reports are available for online members only.*
- **Credit Monitoring:** Actively monitors Experian, Equifax and Transunion files for indicators of fraud.
- **Identity Restoration:** Identity Restoration specialists are immediately available to help you address credit and non-credit related fraud.
- **Experian IdentityWorks ExtendCARE™:** You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **Up to \$1 Million Identity Theft Insurance**:** Provides coverage for certain costs and unauthorized electronic fund transfers.

If you believe there was fraudulent use of your information and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent at 1-877-288-8057. If, after discussing your situation with an agent, it is determined that Identity Restoration support is needed, then an Experian Identity Restoration agent is available to work with you to investigate and resolve each incident of fraud that occurred (including, as appropriate, helping you with contacting credit grantors to dispute charges and close accounts; assisting you in placing a freeze on your credit file with the three major credit bureaus; and assisting you with contacting government agencies to help restore your identity to its proper condition).

Please note that this Identity Restoration support is available to you for one year from the date of this letter and does not require any action on your part at this time. The Terms and Conditions for this offer are located at www.ExperianIDWorks.com/restoration. You will also find self-help tips and information about identity protection at this site.

EXHIBIT 2



April 14, 2021

Re: Notice of Data Breach

Dear Richard Archibeque,

I am writing to inform you of a data security incident recently experienced by FPI Management ("FPI") that may have impacted your personal information. FPI takes the privacy and security of all information within its possession very seriously, which is why I am writing to notify you of this incident and to inform you of steps that can be taken to help safeguard your information.

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

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

What Information Was Involved: The incident may have impacted your 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, and / or medical information.

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

In connection with this incident, and out of an abundance of caution, FPI is offering complimentary identity theft protection services through Experian IdentityWorksSM. Enrollment instructions can be found on the next page of this letter.

What You Can Do: While we are not aware of any misuse of potentially impacted information in connection with the incident, as a precautionary measure, we recommend that you remain vigilant and review your account statements and credit reports closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company that maintains your account. You should also promptly report any fraudulent activity or any suspected incidents of identity theft to proper law enforcement authorities.

EXHIBIT 3



CALIFORNIA CONSUMER PRIVACY ACT

The CCPA provides consumers (California residents) with specific rights regarding their personal information. This section describes your CCPA rights and explains how to **exercise** those rights.

Access to Specific Information and Data Portability Rights

You have the right to request that FPI Management disclose certain information to you about our collection and use of your personal information over the past 12 months. Once we receive and confirm your verifiable consumer request, we will disclose to you:

- The categories of personal information we collected about you.
- The categories of sources for the personal information we collected about you.
- Our business or commercial purpose for collecting that personal information.
- The categories of third parties with whom we share that personal information.
- The specific pieces of personal information we collected about you (also called a data portability request).
- If we disclosed your personal information for a business purpose, the personal information categories that each category of recipient obtained.

Only you, or a person registered with the California Secretary of State that you authorize to act on your behalf, may make a verifiable consumer request related to your personal information. You may also make a verifiable consumer request on behalf of your minor child. You may only make a verifiable consumer request for access or data portability twice within a 12-month period. **The verifiable consumer request must:**

- Provide sufficient information that allows us to reasonably verify you are the person about whom we collected personal information or an authorized representative.
- Describe your request with sufficient detail that allows us to properly understand, evaluate, and respond to it.

We Don't Sell Consumer, Tenant, Employee, or Property Owner Data

FPI Management **does not sell** your personal information to anyone, and retains your data in our systems for the strict purpose of providing our property management services, and as required by County, State, and Federal regulations.

All the information we collect, and as described in our **privacy policy**, is used strictly for providing services to tenants and property owners. We disclose personal information to third parties strictly for business purposes relating to property management, and we never disclose or sell your personal information to third parties for purposes outside of conducting FPI's business of property management without disclosures and written consent from you, the individual. Under certain circumstances, FPI Management is required to release or share your information when it is necessary to comply with law enforcement, governmental mandate, court order, subpoena, or other legal requirement, if appropriate, for your protection or in connection with an investigation or prosecution of possible unlawful activity

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.

Age Restrictions in our business activities

Our website, nor our property management services, are directed at children under age 13, and we certainly would not sell or disclose the personal information of anyone we know is under age 13 in compliance with **Children's Online Privacy Protection Act**, without affirmative authorization as required by the law, and other state and federal regulations.

Right to not be Discriminated Against for Exercising your Rights under CCPA

We will not discriminate against you for exercising any of your CCPA rights. Unless permitted by the CCPA, we will not:

- Deny you goods or services.
- Charge you different prices or rates for goods or services, including through granting discounts or other benefits, or imposing penalties.
- Provide you a different level or quality of goods or services.
- Suggest that you may receive a different price or rate for goods or services or a different level or quality of goods or services.

Here's how the CCPA defines "personal information":

"Personal information" means information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household.

("Household" is defined by the CCPA regulations as "a person or group of people occupying a single dwelling.")

Personal information includes, but is not limited to, the following if it identifies, relates to, describes, is capable of being associated with, or could be reasonably linked, directly or indirectly, with a particular consumer or household:

(A) Identifiers such as a real name, alias, postal address, unique personal identifier, online identifier, Internet Protocol address, email address, account name, social security number, driver's license number, passport number, or other similar identifiers.

(B) Any categories of personal information described in subdivision (e) of Section 1798.80.

[Section 1798.80 states: "Personal information" means any information that identifies, relates to, describes, or is capable of being associated with, a particular individual, including, but not limited to, his or her name, signature, social security number, physical characteristics or description, address, telephone number, passport number, driver's license or state identification card number, insurance policy number, education, employment, employment history, bank account number, credit card number, debit card number, or any other financial information, medical information, or health

insurance information. 'Personal information' does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records."]

(C) Characteristics of protected classifications under California or federal law.

(D) Commercial information, including records of personal property, products or services purchased, obtained, or considered, or other purchasing or consuming histories or tendencies.

(E) Biometric information.

(F) Internet or other electronic network activity information, including, but not limited to, browsing history, search history, and information regarding a consumer's interaction with an Internet Web site, application, or advertisement.

(G) Geolocation data.

(H) Audio, electronic, visual, thermal, olfactory, or similar information. (I) Professional or employment-related information:

(J) Education information, defined as information that is not publicly available personally identifiable information as defined in the Family Educational Rights and Privacy Act (20 U.S.C. §1232g and 34 C.F.R. Part 99).

(K) Inferences drawn from any of the information identified in this subdivision to create a profile about a consumer reflecting the consumer's preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes.

Exclusions and Exceptions of Personal Information

The CCPA also **excludes** some things from the definition of "personal information":

- Publicly available information
- Aggregate consumer information
- De-identified information

The **CCPA** defines those exclusions as follows:

Publicly Available Information

For these purposes, "publicly available" means information that is lawfully made available from federal, state, or local government records, if any conditions associated with such information.

"Publicly available" does not mean biometric information collected by a business about a consumer without the consumer's knowledge. Information is not "publicly available" if that data is used for a purpose that is not compatible with the purpose for which the data is maintained and made available in the government records or for which it is publicly maintained. "Publicly available" does not include consumer information that is de-identified or aggregate consumer information.

Aggregate Consumer Information

"Aggregate consumer information" means information that relates to a group or category of consumers, from which individual consumer identities have been removed, that is not linked or reasonably linkable to any consumer or household, including via a device. "Aggregate consumer information" does not mean one or more individual consumer records that have been deidentified.

De-Identified Information

"Deidentified information" means information that cannot reasonably identify, relate to, describe, be capable of being associated with, or be linked, directly or indirectly, to a particular consumer, provided that a business that uses deidentified information: (1) Has implemented technical safeguards that prohibit reidentification of the consumer to whom the information may pertain. (2) Has implemented business processes that specifically prohibit reidentification of the information. (3) Has implemented business processes to prevent inadvertent release of deidentified information. (4) Makes no attempt to reidentify the information.

Exercising Your Rights Under CCPA

You have a right to submit what the CCPA calls a "verifiable consumer request," to confirm the above, a request to opt-out of information collection, inquire as to the categories of data stored and shared about you, understand the business purpose for the collection of certain categories of data, obtain a copy of the data FPI has stored about you, and/or a request to delete any personal information we may have about you.

- **Complete the online request form [HERE](#)**
- **Email privacy@fpimgt.com,**
- **By calling 1-800-438-4374**

We authenticate all requests – that is, we make sure it's you and not someone else – by requiring you to provide additional specific information to prove your identity. If you decide to

use what the CCPA calls an "authorized agent" to submit your request, your agent must use your name, email, and phone number, since that's the only means we have to authenticate your request. **FPI Management's Department of Information Security** will reach out to you directly to verify your identity in order to complete your request.

Please visit this page from a desktop browser to complete the data access request form and FPI Management will respond within 45 days.

*** Since we're required to track and report statistics regarding the number of requests we receive annually, we will do so and report the results in January 2021.*

Contacting FPI Management

If there are any questions regarding this privacy policy, you may contact us using the information below:

FPI Management | 800 Iron Point Road | Folsom | CA 95630 | USA | FPIMGT.com | 916-357-5300

Contact Us

Last Edited on 2020-03-01

FPI MANAGEMENT

800 Iron Point Road Folsom, CA 95630

Connect With Us



Contact Us

- [Contact](#)
- [Customer Experience](#)
- [Request a Proposal](#)

Resources

- [CCPA Policy](#)
- [Disclosures & Licenses](#)
- [Employee Resources](#)
- [FPI Blog](#)
- [Privacy Policy](#)
- [Resident Services](#)

Exhibit B

1 MICHAEL F. RAM (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 mram@forthepeople.com

9 M. ANDERSON BERRY (SBN 262879)
10 GREGORY HAROUTUNIAN (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 aberry@justice4you.com
18 gharoutunian@justice4you.com

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

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

Attorneys for Plaintiff and the Putative Class

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.

**DECLARATION OF JOHN A.
YANCHUNIS IN SUPPORT OF MOTION
TO AMEND COMPLAINT**

I, John A. Yanchunis, pursuant to Cal Code of Civil Procedure 2015.5, declare as follows:

1. I submit this declaration in support of Plaintiff's Motion to Amend Complaint.

2. I have personal knowledge of the matters stated herein and if called upon, I could and would competently testify.

3. I am a partner at Morgan & Morgan and lead its class action practice department and I am one of the counsel of record for Plaintiff in this matter. I am admitted to practice *pro hac vice* in this matter.

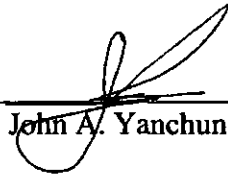
4. The effect of the amendment is to allow Plaintiff, on behalf of himself and others similarly situated, to seek statutory damages under the CCPA.

5. The amendment is necessary and proper to allow Plaintiff to seek damages under the CCPA.

6. The facts giving rise to the amended allegations were discovered when Plaintiff received Defendant's written response to Plaintiff's written notice.

7. The amendment was not made earlier because at the time Plaintiff filed the complaint Plaintiff had not yet received Defendant's written response to Plaintiff's written notice affording Defendant an opportunity to cure its CCPA violations.

1 I declare under penalty of perjury under the laws of the State of California that that foregoing
2 is true and correct. Executed this 9th day of May 2022, at Tampa, Florida.
3
4

5 By: 
6 John A. Yanchunis
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28