

1 SCOTT EDELSBERG
CA Bar No. 330990
2 *scott@edelsberglaw.com*
EDELSBERG LAW, P.A.
3 1925 Century Park E #1700
Los Angeles, CA 90067
4 Telephone: 305.975.3320
Attorney for Plaintiff and Proposed Class

5 (additional counsel listed on signature page)

6
7 **UNITED STATES DISTRICT COURT**
NORTHERN DISTRICT OF CALIFORNIA

8 **DANIEL JIMENEZ JR**, individually,
9 and on behalf of all others similarly
situated,

10 Plaintiff,

11 vs.

12 **OE FEDERAL CREDIT UNION**,

13 Defendant.

Case No. _____

CLASS ACTION COMPLAINT

- 1. Negligence
- 2. Negligence *per se*
- 3. Breach of Implied Contract
- 4. Invasion of Privacy
- 5. Breach of Fiduciary Duty
- 6. Violation of the California Unfair Competition Law
- 7. Violation of the California Consumer Privacy Act
- 8. Violation of the California Consumer Records Act
- 9. Declaratory Judgement

DEMAND FOR JURY TRIAL

18 Plaintiff Daniel Jimenez Jr., individually, and on behalf of all others similarly
19 situated, brings this Class Action Complaint (“Complaint”) against Defendant OE
20

1 Federal Credit Union (“OEFCU” or “Defendant”), to obtain damages, restitution,
2 and injunctive relief for the Class, as defined below, from Defendant. Plaintiff
3 makes the following allegations on information and belief, except as to his own
4 actions, which are made on personal knowledge, the investigation of counsel, and
5 the facts that are a matter of public record.

6 INTRODUCTION

7 1. This class action arises out of the recent targeted ransomware attack
8 and data breach (“Data Breach”) on Defendant’s network that resulted in
9 unauthorized access to the highly sensitive data. As a result of the Data Breach,
10 Class Members suffered ascertainable losses in the form of the benefit of their
11 bargain, out-of-pocket expenses, and the value of their time reasonably incurred to
12 remedy or mitigate the effects of the attack, emotional distress, and the present risk
13 of imminent harm caused by the compromise of their sensitive personal
14 information.

15 2. Upon information and belief, the specific information compromised in
16 the Data Breach includes, but is not limited to, personally identifiable information
17 (“PII”), such as full name, Social Security number, driver’s license or government
18

1 ID number¹.

2 3. Upon information and belief, up to and through April 2024, Defendant
3 obtained the PII of Plaintiff and Class Members and stored that PII, unencrypted,
4 in an Internet-accessible environment on Defendant's network, from which
5 unauthorized actors used an extraction tool to retrieve sensitive PII belonging to
6 Plaintiff and Class Members.

7 4. Plaintiff's and Class Members' PII—which were entrusted to
8 Defendant, their officials, and agents—were compromised and unlawfully accessed
9 due to the Data Breach.

10 5. Plaintiff brings this class action lawsuit on behalf of those similarly
11 situated to address Defendant's inadequate safeguarding of Plaintiff's and Class
12 Members' PII that Defendant collected and maintained, and for Defendant's failure
13 to provide timely and adequate notice to Plaintiff and other Class Members that
14 their PII had been subject to the unauthorized access of an unknown, unauthorized
15 party.

16 6. Defendant maintained the PII in a negligent and/or reckless manner.
17 In particular, the PII was maintained on Defendant's computer system and network

18
19
20 ¹ Notice of Data Breach ("Notice") attached hereto as **Exhibit A**.

1 in a condition vulnerable to cyberattacks. Upon information and belief, the
2 mechanism of the cyberattack and potential for improper disclosure of Plaintiff's
3 and Class Members' PII was a known risk to Defendant, and thus Defendant was
4 on notice that failing to take steps necessary to secure the PII from those risks left
5 that property in a dangerous condition.

6 7. In addition, upon information and belief, Defendant and its employees
7 failed to properly monitor the computer network, IT systems, and integrated service
8 that housed Plaintiff's and Class Members' PII.

9 8. Defendant's failure to safeguard its clients PII is particularly heinous
10 in light of the fact that Defendant suffered the data breach between August 19, 2023
11 and October 29, 2023, *a period lasting more than two months*, about which it
12 notified its customers several months later in April 2024.

13 9. Plaintiff's and Class Members' identities are now at risk because of
14 Defendant's negligent conduct because the PII that Defendant collected and
15 maintained is now in the hands of malicious cybercriminals. The risks to Plaintiff
16 and Class Members will remain for their respective lifetimes.

17 10. Defendant failed to provide timely, accurate and adequate notice to
18 Plaintiff and Class Members. Plaintiff and Class Members' knowledge about the
19 PII Defendant lost, as well as precisely what type of information was unencrypted
20

1 and in the possession of unknown third parties, was unreasonably delayed by
2 Defendant's failure to warn impacted persons immediately upon learning of the
3 Data Breach.

4 11. As remediation for allowing Plaintiff's and Class Members' PII to be
5 acquired by an unauthorized third-party, Defendant has stated that "we are
6 providing you with access to a complimentary 12-month membership of Experian
7 IdentityWorks."² To date, Defendant has not contacted or offered any remediation
8 to the victims of this Data Breach, but this assurance serves as tacet
9 acknowledgement of the harm and elevated risk that Plaintiff and class members
10 now face as a result of Defendant's acts and omissions.

11 12. Indeed, armed with the PII accessed in the Data Breach, data thieves
12 can commit a variety of crimes including opening new financial accounts in Class
13 Members' names, taking out loans in Class Members' names, using Class
14 Members' names to obtain medical services, using Class Members' information to
15 target other phishing and hacking intrusions using Class Members' information to
16 obtain government benefits, filing fraudulent tax returns using Class Members'
17 information, obtaining driver's licenses in Class Members' names but with another

18
19
20 ² *Id.*

1 person's photograph, and giving false information to police during an arrest.

2 13. As a result of the Data Breach, Plaintiff and Class Members have been
3 exposed to a present, heightened and imminent risk of fraud and identity theft.
4 Plaintiff and Class Members must now closely monitor their financial accounts to
5 guard against identity theft for the rest of their lives.

6 14. Plaintiff and Class Members may also incur out of pocket costs for
7 purchasing credit monitoring services, credit freezes, credit reports, or other
8 protective measures to deter and detect identity theft.

9 15. By his Complaint, Plaintiff seeks to remedy these harms on behalf of
10 himself and all similarly situated individuals whose PII was accessed during the
11 Data Breach.

12 16. Accordingly, Plaintiff brings claims on behalf of himself and the Class
13 for: (i) negligence, (ii) negligence *per se*, (iii) breach of implied contract (iv)
14 invasion of privacy (v) breach of fiduciary duty, (vi) violations of the California
15 Unfair Competition Law, (vii) violations of the California Consumer Privacy Act,
16 (viii) violations of the California Consumer Records Act and (ix) declaratory
17 judgment. Through these claims, Plaintiff seeks, *inter alia*, damages and injunctive
18 relief, including improvements to Defendant's data security systems and integrated
19 services, future annual audits, and adequate credit monitoring services.
20

1
2 **PARTIES**

3 17. Plaintiff Daniel Jimenez Jr. is a natural person, resident, and citizen of
4 California where he intends to remain. He is a Data Breach victim, being a customer
5 of Defendant.

6 18. Defendant OE Federal Credit Union is a corporation, incorporated
7 under the laws of Nevada, with its principal place of business at 250 North Canyons
8 Parkway, Livermore, California 94551.

9 **JURISDICTION AND VENUE**

10 19. This Court has original jurisdiction over this action under the Class
11 Action Fairness Act, 28 U.S.C. § 1332(d)(2). The amount in controversy exceeds
12 \$5 millions, exclusive of interest and costs, there are more than 100 members in the
13 proposed class, and at least one member of the class is a citizen of a state different
14 from Defendant³.

15 20. This Court has personal jurisdiction over Defendant because
16 Defendant is headquartered in this District and does substantial business in
17

18 _____
19 ³ According to the breach report submitted to the Massachusetts state government, 71
20 Massachusetts residents were impacted in the Data Breach at OE Federal Credit Union. See
<https://www.mass.gov/doc/data-breach-report-2024/download>

1 California.

2 21. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(b) because
3 Defendant's principal places of business is in this District and a substantial part of
4 the events, acts, and omissions giving rise to Plaintiff's claims occurred in this
5 District.

6 **BACKGROUND FACTS**

7 **A. Defendant's Businesses**

8 22. According to Defendant's website "OE Federal is the country's largest
9 labor-based credit union."⁴

10 23. On information and belief, Defendant maintain the PII of current and
11 former customers, including but not limited to:

- 12 a. name;
- 13 b. Social Security number;
- 14 c. Driver's license number or government IDs; and
- 15 d. other information that Defendant may deem necessary to
16 provide its services.

17 24. Plaintiff and Class Members directly or indirectly entrusted Defendant
18

19 ⁴ A Union Proud History, <https://oefederal.org/about/about-oe/history/> (last accessed May 8,
20 2024)

1 with sensitive and confidential PII, which includes information that is static, does
2 not change, and can be used to commit myriad financial crimes.

3 25. Because of the highly sensitive and personal nature of the information
4 Defendant acquires, stores, and has access to, Defendant, upon information and
5 belief, promised to, among other things: keep PII private; comply with industry
6 standards related to data security and PII; inform individuals of their legal duties
7 and comply with all federal and state laws protecting PII; only use and release PII
8 for reasons that relate to medical care and treatment; and provide adequate notice
9 to impacted individuals if their PII is disclosed without authorization.

10 26. By obtaining, collecting, using, and deriving a benefit from Plaintiff's
11 and Class Members' PII, Defendant assumed legal and equitable duties and knew
12 or should have known that it was responsible for protecting Plaintiff's and Class
13 Members' PII from unauthorized disclosure.

14 27. Plaintiff and the Class Members have taken reasonable steps to
15 maintain the confidentiality of their PII.

16 28. Plaintiff and the Class Members relied on Defendant to implement and
17 follow adequate data security policies and protocols, to keep their PII confidential
18 and securely maintained, to use such PII solely for business purposes, and to
19 prevent the unauthorized disclosures of the PII.
20

1 //

2 **B. Defendant Fails to Safeguard Consumer PII**

3 29. On or around April 30, 2024, Defendant began sending Data Breach
4 Victims a Notice of Data Security Breach letter (“Notice”) informing them that:

5 *What Happened?*

6 On or about October 28, 2023, OEFCU detected unauthorized access
7 to our network as a result of a cybersecurity incident that resulted in the
8 potential exposure of the data we maintain.

9 *What We Are Doing.*

10 Upon learning of this issue, we immediately began efforts to secure our
11 network and commenced a prompt and thorough investigation. As part
12 of our investigation, we have been working very closely with external
13 cybersecurity professionals experienced in handling these types of
14 incidents. After an extensive forensic investigation and document
15 review, we discovered on April 1, 2024, that between approximately
16 August 19, 2023 and October 29, 2023, certain impacted files
17 containing personal information may have been accessed and/or
18 acquired by an unauthorized party.

19 *What Information Was Involved?*

20 The impacted information includes your full name, and Social
21 Security number, driver’s license or government ID number.⁵

30. It is likely the Data Breach was targeted at Defendant due to its status


20 ⁵ Exhibit A.

1 as a financial services provider that collects, creates, and maintains sensitive PII.

2 31. Upon information and belief, the cyberattack was expressly designed
3 to gain access to private and confidential data of specific individuals, including
4 (among other things) the PII of Plaintiff and the Class Members.

5 32. Upon information and belief, and based on the type of cyberattack, it
6 is plausible and likely that Plaintiff's PII was stolen in the Data Breach. Plaintiff
7 further believes his PII was likely subsequently sold on the dark web following the
8 Data Breach, as that is the *modus operandi* of cybercriminals.

9 33. The notorious ransomware group NoEscape claimed responsibility for
10 the cyberattack.

11  **NOESCAPE** | **OEFEDERAL.ORG** | 29 Oct 2023 @ 175 | NEWCOMERS | ARCHIVE

12 **OE FEDERAL CREDIT UNION**
13 250 North Canyons Parkway Livermore, CA 94551
@ oefederal.org
800.877.4444

14 Built on a foundation of union pride, **OE Federal** is the country's largest labor-based credit union. We understand the unique needs of union workers and their families in ways the big banks can't. With more than 100,000 members nationwide across six states and 125 union groups, we're here to help because we're union family, and our family deserves the best.

15 **The company network was successfully encrypted and compromised.**
16 The company's management apparently does not understand the current situation, and decided to remain silent, but we are ready to provide comprehensive evidence that the management is lying, we were on the network for a long time and were able to steal some of the company's most confidential data, for example, **we have more than 11TB of such data as:**
Backups and more than 1TB SQL databases!
Personal data and contacts of employees and management!
Personal data of clients SSN, ID CARD, DL, as well as access to their credit and debit cards CC+EXP+CVV!
The entire history of clients' financial movements from 2020 to September 2023, including daily and monthly reports!
Projects, taxes, loans, contracts, agreements, reports, accounting, data from Branch Sales and hundreds of thousands of other confidential and critically important data.

17 **We advise you not to bring the situation to a critical level and contact us soon is possible.**
18 It's interesting to watch the OFCU blog as they do their best to ensure that their clients are not deceived and that they do not trust the scammers while we have compromised a staggering amount of confidential data directly from their servers! Guys, you have no other path, or you will contact with us and we will make a deal or **we will inflict such damage on you from which you will no longer be able to recover.** And believe us, we know what we are talking about.
19 **Assign a person to the position of negotiator, and tell him to contact us, we will explain everything and help you solve this problem.**
20 **Time is running out.**

21

1 34. Defendant had a duty to adopt reasonable measures to protect
2 Plaintiff's and Class Members' PII from involuntary disclosure to third parties.

3 35. Because of the Data Breach, data thieves were able to gain access to
4 Defendant's private systems between approximately August 19, 2023 and October
5 29, 2023, a period of time lasting more than two months, and were able to
6 compromise, access, and acquire the protected PII of Plaintiff and Class Members.

7 36. Defendant had obligations created by contract, industry standards,
8 common law, and its own promises and representations made to Plaintiff and Class
9 Members to keep their PII confidential and to protect them from unauthorized
10 access and disclosure.

11 37. Plaintiff and the Class Members reasonably relied (directly or
12 indirectly) on Defendant's sophistication to keep their sensitive PII confidential; to
13 maintain proper system security; to use this information for business purposes only;
14 and to make only authorized disclosures of their PII.

15 38. Plaintiff's and Class Members' unencrypted, unredacted PII was
16 compromised due to Defendant's negligent and/or careless acts and omissions, and
17 due to the utter failure to protect Class Members' PII. Criminal hackers obtained
18 their PII because of its value in exploiting and stealing the identities of Plaintiff and
19 Class Members. The risks to Plaintiff and Class Members will remain for their
20

1 respective lifetimes.

2 **C. The Data Breach was a Foreseeable Risk and Defendant were on Notice**

3 39. Defendant's data security obligations were particularly important
4 given the substantial increase in cyberattacks and/or data breaches in industries
5 holding significant amounts of PII preceding the date of the breach.

6 40. In light of recent high profile data breaches at other financial services
7 companies, Defendant knew or should have known that their electronic records and
8 PII they maintained would be targeted by cybercriminals and ransomware attack
9 groups.

10 41. Defendant knew or should have known that these attacks were
11 common and foreseeable.

12 42. In 2021, a record 1,862 data breaches occurred, resulting in
13 approximately 293,927,708 sensitive records being exposed, a 68% increase from
14 2020.⁶ The 330 reported breaches reported in 2021 exposed nearly 30 million
15 sensitive records (28,045,658), compared to only 306 breaches that exposed nearly
16 10 million sensitive records (9,700,238) in 2020.⁷

17 43. Therefore, the increase in such attacks, and attendant risk of future
18

19 ⁶ See 2021 Data Breach Annual Report (ITRC, Jan. 2022) (available at
20 <https://notified.idtheftcenter.org/s/>), at 6.

⁷ *Id.*

1 attacks, was widely known to the public and to anyone in Defendant’s industry,
2 including Defendant.

3 **D. Defendant Fails to Comply with FTC Guidelines**

4 44. The Federal Trade Commission (“FTC”) has promulgated numerous
5 guides for businesses which highlight the importance of implementing reasonable
6 data security practices. According to the FTC, the need for data security should be
7 factored into all business decision-making.

8 45. In 2016, the FTC updated its publication, *Protecting Personal*
9 *Information: A Guide for Business*, which established cyber-security guidelines for
10 businesses. The guidelines note that businesses should protect the personal
11 customer information that they keep; properly dispose of personal information that
12 is no longer needed; encrypt information stored on computer networks; understand
13 its network’s vulnerabilities; and implement policies to correct any security
14 problems.⁸ The guidelines also recommend that businesses use an intrusion
15 detection system to expose a breach as soon as it occurs; monitor all incoming
16 traffic for activity indicating someone is attempting to hack the system; watch for
17 large amounts of data being transmitted from the system; and have a response plan
18

19 ⁸ *Protecting Personal Information: A Guide for Business*, Federal Trade Commission (2016).
20 Available at https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last visited May 8, 2024).

1 ready in the event of a breach.⁹

2 46. The FTC further recommends that companies not maintain PII longer
3 than is needed for authorization of a transaction; limit access to sensitive data;
4 require complex passwords to be used on networks; use industry-tested methods
5 for security; monitor for suspicious activity on the network; and verify that third-
6 party service providers have implemented reasonable security measures.

7 47. The FTC has brought enforcement actions against businesses for
8 failing to adequately and reasonably protect customer data, treating the failure to
9 employ reasonable and appropriate measures to protect against unauthorized access
10 to confidential consumer data as an unfair act or practice prohibited by Section 5 of
11 the Federal Trade Commission Act (“FTCA”), 15 U.S.C. § 45. Orders resulting
12 from these actions further clarify the measures businesses must take to meet their
13 data security obligations.

14 48. These FTC enforcement actions include actions against financial
15 institutions like Defendant.

16 49. Defendant failed to properly implement basic data security practices.

17 50. Defendant’s failure to employ reasonable and appropriate measures to
18 protect against unauthorized access to customers and other impacted individuals’

19
20 ⁹ *Id.*

1 PII constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15
2 U.S.C. § 45.

3 51. Defendant was at all times fully aware of their obligation to protect the
4 PII. Defendant was also aware of the significant repercussions that would result
5 from their failure to do so.

6 **E. Defendant Fails to Comply with Industry Standards**

7 52. As shown above, experts studying cyber security routinely identify
8 financial institutions as being particularly vulnerable to cyberattacks because of the
9 value of the PII which they collect and maintain.

10 53. Several best practices have been identified that at a minimum should
11 be implemented by financial institutions like Defendant, including but not limited
12 to: educating all employees; strong passwords; multi-layer security, including
13 firewalls, anti-virus, and anti-malware software; encryption, making data
14 unreadable without a key; multi-factor authentication; backup data; and limiting
15 which employees can access sensitive data.

16 54. Other best cybersecurity practices that are standard in the financial
17 industry include installing appropriate malware detection software; monitoring and
18 limiting the network ports; protecting web browsers and email management
19 systems; setting up network systems such as firewalls, switches and routers;
20

1 monitoring and protection of physical security systems; protection against any
2 possible communication system; training staff regarding critical points.

3 55. Defendant failed to meet the minimum standards of any of the
4 following frameworks: the NIST Cybersecurity Framework Version 1.1 (including
5 without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7,
6 PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-
7 7, DE.CM-8, and RS.CO-2), and the Center for Internet Security’s Critical Security
8 Controls (CIS CSC), which are all established standards in reasonable cybersecurity
9 readiness.

10 56. These foregoing frameworks are existing and applicable industry
11 standards in the financial industry, and Defendant failed to comply with these
12 accepted standards, thereby opening the door to the cyber incident and causing the
13 data breach.

14 **F. Defendant’s Breach**

15 57. Defendant breached its obligations to Plaintiff and Class Members
16 and/or was otherwise negligent and reckless because it failed to properly maintain
17 and safeguard its computer systems and website’s application flow. Defendant’s
18 unlawful conduct includes, but is not limited to, the following acts and/or
19 omissions:
20

- 1 a. failing to maintain an adequate data security system to reduce
- 2 the risk of data breaches and cyber-attacks;
- 3 b. failing to adequately protect PII;
- 4 c. failing to properly monitor their own data security systems for
- 5 existing intrusions;
- 6 d. failing to ensure that their vendors with access to their computer
- 7 systems and data employed reasonable security procedures;
- 8 e. failing to ensure the confidentiality and integrity of electronic
- 9 PII it created, received, maintained, and/or transmitted;
- 10 f. failing to implement technical policies and procedures for
- 11 electronic information systems that maintain electronic PII to
- 12 allow access only to those persons or software programs that
- 13 have been granted access rights;
- 14 g. failing to implement policies and procedures to prevent, detect,
- 15 contain, and correct security violations;
- 16 h. failing to implement procedures to review records of
- 17 information system activity regularly, such as audit logs, access
- 18 reports, and security incident tracking reports;
- 19 i. failing to protect against reasonably anticipated threats or
- 20

1 hazards to the security or integrity of electronic PII;

2 j. failing to train all members of their workforces effectively on
3 the policies and procedures regarding PII;

4 k. failing to render the electronic PII it maintained unusable,
5 unreadable, or indecipherable to unauthorized individuals;

6 l. failing to comply with FTC guidelines for cybersecurity, in
7 violation of Section 5 of the FTC Act;

8 m. failing to adhere to industry standards for cybersecurity as
9 discussed above; and,

10 n. otherwise breaching their duties and obligations to protect
11 Plaintiff's and Class Members' PII.

12 //

13 58. Defendant negligently and unlawfully failed to safeguard Plaintiff's
14 and Class Members' PII by allowing cyberthieves to access Defendant's online
15 insurance application flow, which provided unauthorized actors with unsecured and
16 unencrypted PII.

17 59. Accordingly, as outlined below, Plaintiff and Class Members now face
18 a present, increased risk of fraud and identity theft. In addition, Plaintiff and the
19 Class Members also lost the benefit of the bargain they made with Defendant.

1 **G. Data Breaches Cause Disruption and Increased Risk of Fraud and**
2 **Identity Theft**

3 60. Cyberattacks and data breaches at financial institutions like Defendant
4 are especially problematic because they can negatively impact the overall daily
5 lives of individuals affected by the attack.

6 61. The United States Government Accountability Office released a report
7 in 2007 regarding data breaches (“GAO Report”) in which it noted that victims of
8 identity theft will face “substantial costs and time to repair the damage to their good
9 name and credit record.”¹⁰

10 62. That is because any victim of a data breach is exposed to serious
11 ramifications regardless of the nature of the data. Indeed, the reason criminals steal
12 personally identifiable information is to monetize it. They do this by selling the
13 spoils of their cyberattacks on the black market to identity thieves who desire to
14 extort and harass victims, take over victims’ identities in order to engage in illegal
15 financial transactions under the victims’ names. Because a person’s identity is akin
16 to a puzzle, the more accurate pieces of data an identity thief obtains about a person,
17 the easier it is for the thief to take on the victim’s identity, or otherwise harass or

18
19 ¹⁰ See U.S. GOV. ACCOUNTING OFFICE, GAO-07-737, *Personal Information: Data Breaches Are*
20 *Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is*
Unknown (2007) <https://www.gao.gov/new.items/d07737.pdf>.

1 track the victim. For example, armed with just a name and date of birth, a data thief
2 can utilize a hacking technique referred to as “social engineering” to obtain even
3 more information about a victim’s identity, such as a person’s login credentials or
4 Social Security number. Social engineering is a form of hacking whereby a data
5 thief uses previously acquired information to manipulate individuals into disclosing
6 additional confidential or personal information through means such as spam phone
7 calls and text messages or phishing emails.

8 63. The FTC recommends that identity theft victims take several steps to
9 protect their personal and financial information after a data breach, including
10 contacting one of the credit bureaus to place a fraud alert (consider an extended
11 fraud alert that lasts for 7 years if someone steals their identity), reviewing their
12 credit reports, contacting companies to remove fraudulent charges from their
13 accounts, placing a credit freeze on their credit, and correcting their credit reports.¹¹

14 64. Identity thieves use stolen personal information such as Social
15 Security numbers for a variety of crimes, including credit card fraud, phone or
16 utilities fraud, and bank/finance fraud.

17 65. Identity thieves can also use Social Security numbers to obtain a
18

19
20 ¹¹ See *IdentityTheft.gov*, FEDERAL TRADE COMMISSION, <https://www.identitytheft.gov/Steps> (last
accessed May 8, 2024).

1 driver’s license or official identification card in the victim’s name but with the
2 thief’s picture; use the victim’s name and Social Security number to obtain
3 government benefits; or file a fraudulent tax return using the victim’s information.
4 In addition, identity thieves may obtain a job using the victim’s Social Security
5 number, rent a house or receive medical services in the victim’s name, and may
6 even give the victim’s personal information to police during an arrest resulting in
7 an arrest warrant being issued in the victim’s name.

8 66. Moreover, theft of PII is also gravely serious because PII is an
9 extremely valuable property right.¹²

10 67. Its value is axiomatic, considering the value of “big data” in corporate
11 America and the fact that the consequences of cyber thefts include heavy prison
12 sentences. Even this obvious risk to reward analysis illustrates beyond doubt that
13 PII has considerable market value.

14 68. It must also be noted there may be a substantial time lag – measured
15 in years -- between when harm occurs and when it is discovered, and also between
16 when PII is stolen and when it is used.

18
19 ¹² See, e.g., John T. Soma, et al, *Corporate Privacy Trend: The “Value” of Personally Identifiable*
20 *Information (“PII”) Equals the “Value” of Financial Assets*, 15 RICH. J.L. & TECH. 11, at *3-4
(2009) (“PII, which companies obtain at little cost, has quantifiable value that is rapidly reaching
a level comparable to the value of traditional financial assets.”) (citations omitted).

1 69. According to the U.S. Government Accountability Office, which
2 conducted a study regarding data breaches:

3 [L]aw enforcement officials told us that in some cases, stolen
4 data may be held for up to a year or more before being used to
5 commit identity theft. Further, once stolen data have been sold
6 or posted on the Web, fraudulent use of that information may
7 continue for years. As a result, studies that attempt to measure
8 the harm resulting from data breaches cannot necessarily rule
9 out all future harm.¹³

10 70. PII is such a valuable commodity to identity-thieves that once the
11 information has been compromised, criminals often trade the information on the
12 “cyber black-market” for years.

13 71. There is a strong probability that entire batches of stolen information
14 have been dumped on the black market and are yet to be dumped on the black
15 market, meaning Plaintiff and Class Members are at an increased risk of fraud and
16 identity theft for many years into the future.

17 72. Thus, Plaintiff and Class Members must vigilantly monitor their
18 financial and medical accounts for many years to come.

19 73. PII can sell for as much as \$363 per record according to the Infosec

20 ¹³ GAO Report, at p. 21.

1 Institute.¹⁴ PII is particularly valuable because criminals can use it to target victims
2 with frauds and scams. Once PII is stolen, fraudulent use of that information and
3 damage to victims may continue for many years.

4 74. For example, the Social Security Administration has warned that
5 identity thieves can use an individual's Social Security number to apply for
6 additional credit lines.¹⁵ Such fraud may go undetected until debt collection calls
7 commence months, or even years, later. Stolen Social Security Numbers also make
8 it possible for thieves to file fraudulent tax returns, file for unemployment benefits,
9 or apply for a job using a false identity.¹⁶ Each of these fraudulent activities is
10 difficult to detect. An individual may not know that their Social Security Number
11 was used to file for unemployment benefits until law enforcement notifies the
12 individual's employer of the suspected fraud. Fraudulent tax returns are typically
13 discovered only when an individual's authentic tax return is rejected.

14 75. Moreover, it is not an easy task to change or cancel a stolen Social
15 Security number.

16 76. An individual cannot obtain a new Social Security number without
17

18 ¹⁴ See Ashiq Ja, *Hackers Selling Healthcare Data in the Black Market*, INFOSEC (July 27, 2015),
19 [https://resources.infosecinstitute.com/topic/hackers-selling-healthcare-data-in-the-black-](https://resources.infosecinstitute.com/topic/hackers-selling-healthcare-data-in-the-black-market/)
20 [market/](https://resources.infosecinstitute.com/topic/hackers-selling-healthcare-data-in-the-black-market/). (last accessed May 8, 2024).

¹⁵ *Identity Theft and Your Social Security Number*, SOCIAL SECURITY ADMINISTRATION (2018) at
1, <https://www.ssa.gov/pubs/EN-05-10064.pdf> (last accessed May 8, 2024).

¹⁶ *Id* at 4.

1 significant paperwork and evidence of actual misuse. Even then, a new Social
2 Security number may not be effective, as “[t]he credit bureaus and banks are able
3 to link the new number very quickly to the old number, so all of that old bad
4 information is quickly inherited into the new Social Security number.”¹⁷

5 77. This data, as one would expect, demands a much higher price on the
6 black market. Martin Walter, senior director at cybersecurity firm RedSeal,
7 explained, “[c]ompared to credit card information, personally identifiable
8 information and Social Security Numbers are worth more than 10x on the black
9 market.”¹⁸

10 78. Because of the value of its collected and stored data, the financial
11 industry has experienced disproportionately higher numbers of data theft events than
12 other industries.

13 79. For this reason, Defendant knew or should have known about these
14 dangers and strengthened its data and email handling systems accordingly.
15 Defendant was put on notice of the substantial and foreseeable risk of harm from a
16 data breach, yet Defendant failed to properly prepare for that risk.

17
18 ¹⁷ Brian Naylor, *Victims of Social Security Number Theft Find It’s Hard to Bounce Back*, NPR
(Feb. 9, 2015), [http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-
has-millions-worrying-about-identity-theft](http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millions-worrying-about-identity-theft).

19 ¹⁸ Tim Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card
20 Numbers*, COMPUTER WORLD (Feb. 6, 2015), [http://www.itworld.com/article/2880960/anthem-
hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html](http://www.itworld.com/article/2880960/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html).

1 **H. Plaintiff's and Class Members' Damages**

2 80. To date, Defendant has done nothing to provide Plaintiff and the Class
3 Members with relief for the damages they have suffered as a result of the Data
4 Breach.

5 81. Defendant has merely offered Plaintiff and Class Members
6 complimentary fraud and identity monitoring services for up to twelve months, but
7 this does nothing to compensate them for damages incurred and time spent dealing
8 with the Data Breach.

9 82. Plaintiff and Class Members have been damaged by the compromise
10 of their PII in the Data Breach.

11 83. Plaintiff and Class Members' PII was compromised in the Data Breach
12 and are now in the hands of the cybercriminals who accessed Defendant's software
13 maintaining PII. This PII was acquired by some unauthorized, unidentified third-
14 party threat actor.

15 84. Since learning of the Data Breach, Plaintiff has spent time dealing with
16 the impact of the Data Breach, valuable time Plaintiff otherwise would have spent
17 on other activities, including but not limited to work and/or recreation.

18 85. Due to the Data Breach, Plaintiff anticipates spending considerable
19 time and money on an ongoing basis to try to mitigate and address harms caused
20

1 by the Data Breach. This includes changing passwords, cancelling credit and debit
2 cards, and monitoring their accounts for fraudulent activity.

3 86. Plaintiff's PII was compromised as a direct and proximate result of the
4 Data Breach.

5 87. As a direct and proximate result of Defendant's conduct, Plaintiff and
6 Class Members have been placed at a present, imminent, immediate, and continuing
7 increased risk of harm from fraud and identity theft.

8 88. As a direct and proximate result of Defendant's conduct, Plaintiff and
9 Class Members have been forced to expend time dealing with the effects of the
10 Data Breach.

11 89. Plaintiff and Class Members face substantial risk of out-of-pocket
12 fraud losses such as loans opened in their names, medical services billed in their
13 names, tax return fraud, utility bills opened in their names, credit card fraud, and
14 similar identity theft.

15 90. Plaintiff and Class Members face substantial risk of being targeted for
16 future phishing, data intrusion, and other illegal schemes based on their PII as
17 potential fraudsters could use that information to more effectively target such
18 schemes to Plaintiff and Class Members.

19 91. Plaintiff and Class Members may also incur out-of-pocket costs for
20

1 protective measures such as credit monitoring fees, credit report fees, credit freeze
2 fees, and similar costs directly or indirectly related to the Data Breach.

3 92. Plaintiff and Class Members also suffered a loss of value of their PII
4 when it was acquired by cyber thieves in the Data Breach. Numerous courts have
5 recognized the propriety of loss of value damages in related cases.

6 93. Plaintiff and Class Members were also damaged via benefit-of-the-
7 bargain damages. Plaintiff and Class Members overpaid for a service that was
8 intended to be accompanied by adequate data security that complied with industry
9 standards but was not. Part of the price Plaintiff and Class Members paid to
10 Defendant was intended to be used by Defendant to fund adequate security of
11 Defendant's systems and Plaintiff's and Class Members' PII. Thus, Plaintiff and
12 Class Members did not get what they paid for and agreed to.

13 94. Plaintiff and Class Members have spent and will continue to spend
14 significant amounts of time to monitor their financial accounts and sensitive
15 information for misuse.

16 95. Plaintiff and Class Members have suffered or will suffer actual injury
17 as a direct result of the Data Breach. Many victims suffered ascertainable losses in
18 the form of out-of-pocket expenses and the value of their time reasonably incurred
19 to remedy or mitigate the effects of the Data Breach relating to:
20

- 1 a. reviewing and monitoring sensitive accounts and finding
- 2 fraudulent insurance claims, loans, and/or government benefits
- 3 claims;
- 4 b. purchasing credit monitoring and identity theft prevention;
- 5 c. placing “freezes” and “alerts” with reporting agencies;
- 6 d. spending time on the phone with or at financial institutions,
- 7 healthcare providers, and/or government agencies to dispute
- 8 unauthorized and fraudulent activity in their name;
- 9 e. contacting financial institutions and closing or modifying
- 10 financial accounts; and
- 11 f. closely reviewing and monitoring Social Security numbers,
- 12 medical insurance accounts, bank accounts, and credit reports
- 13 for unauthorized activity for years to come.

14 96. Moreover, Plaintiff and Class Members have an interest in ensuring
15 that their PII, which is believed to remain in the possession of Defendant, is
16 protected from further breaches by the implementation of adequate security
17 measures and safeguards, including but not limited to, making sure that the storage
18 of data or documents containing PII is not accessible online and that access to such
19 data is password protected.

1 97. Further, as a result of Defendant’s conduct, Plaintiff and Class
2 Members are forced to live with the anxiety that their PII may be disclosed to the
3 entire world, thereby subjecting them to embarrassment and depriving them of any
4 right to privacy whatsoever.

5 98. As a direct and proximate result of Defendant’s actions and inactions,
6 Plaintiff and Class Members have suffered anxiety, emotional distress, and loss of
7 privacy, and are at an increased risk of future harm.

8 ***Plaintiff Jimenez’s Experience***

9 99. Plaintiff Jimenez provided his information to Defendant as a condition
10 of becoming a customer of Defendant.

11 100. Plaintiff Jimenez is very careful about sharing his sensitive Private
12 Information. Plaintiff Jimenez has never knowingly transmitted unencrypted
13 sensitive PII over the internet or any other unsecured source.

14 101. Plaintiff Jimenez first learned of the Data Breach after receiving a
15 Notice of Data Breach letter from Defendant dated April 30, 2024.

16 102. Based on the information he provided to Defendant, Plaintiff Jimenez
17 has reason to believe that his PII including, but not limited to, his full name, Social
18 Security number, driver’s license or government ID number were compromised in
19 this Data Breach.

1 103. As a result of the Data Breach, Plaintiff Jimenez made reasonable
2 efforts to mitigate the impact of the Data Breach after receiving notice of the Data
3 Breach, including but not limited to researching the Data Breach, reviewing credit
4 reports, financial account statements, and/or medical records for any indications of
5 actual or attempted identity theft or fraud.

6 104. Plaintiff Jimenez has spent significant time and will continue to spend
7 valuable hours for the remainder of his life, that he otherwise would have spent on
8 other activities, including but not limited to work and/or recreation.

9 105. Plaintiff Jimenez suffered actual injury from having his PII
10 compromised as a result of the Data Breach including, but not limited to (a) damage
11 to and diminution in the value of his PII, a form of property that Defendant
12 maintained belonging to Plaintiff Jimenez; (b) violation of his privacy rights; (c) the
13 theft of his PII; and (d) present, imminent and impending injury arising from the
14 increased risk of identity theft and fraud.

15 106. As a result of the Data Breach, Plaintiff Jimenez has also suffered
16 emotional distress as a result of the release of his PII, which he believed would be
17 protected from unauthorized access and disclosure, including anxiety about
18 unauthorized parties viewing, selling, and/or using his PII for purposes of identity
19 theft and fraud. Plaintiff Jimenez is very concerned about identity theft and fraud,
20

1 as well as the consequences of such identity theft and fraud resulting from the Data
2 Breach.

3 107. As a result of the Data Breach, Plaintiff Jiminez anticipates spending
4 considerable time and money on an ongoing basis to try to mitigate and address
5 harms caused by the Data Breach. In addition, Plaintiff will continue to be at
6 present, imminent, and continued increased risk of identity theft and fraud for the
7 remainder of his life.

8 CLASS ACTION ALLEGATIONS

9 108. Plaintiff brings this action on behalf of himself and on behalf of all
10 other persons similarly situated (“the Class”).

11 109. Plaintiff proposes the following Class definition, subject to
12 amendment as appropriate:

13 **All persons identified by Defendant (or its agents or**
14 **affiliates) as being among those individuals impacted by the**
15 **Data Breach, including all who were sent a notice of the**
16 **Data Breach (the “Class”).**

17 //

18 110. Excluded from the Class are Defendant’s officers, directors, and
19 employees; any entity in which Defendant has a controlling interest; and the
20 affiliates, legal representatives, attorneys, successors, heirs, and assigns of
21 Defendant. Excluded also from the Class are members of the judiciary to whom this

1 case is assigned, their families and Members of their staff.

2 111. Plaintiff reserves the right to amend or modify the Class definitions as
3 this case progresses.

4 112. Numerosity. The Members of the Class are so numerous that joinder
5 of all of them is impracticable. While the exact number of Class Members is
6 unknown to Plaintiff at this time, based on information and belief, the Class consists
7 of thousands of individuals whose sensitive data was compromised in the Data
8 Breach.

9 113. Commonality. There are questions of law and fact common to the
10 Class, which predominate over any questions affecting only individual Class
11 Members. These common questions of law and fact include, without limitation:

- 12 a. if Defendant unlawfully used, maintained, lost, or disclosed
13 Plaintiff's and Class Members' PII;
- 14 b. if Defendant failed to implement and maintain reasonable
15 security procedures and practices appropriate to the nature and
16 scope of the information compromised in the Data Breach;
- 17 c. if Defendant's data security systems prior to and during the Data
18 Breach complied with applicable data security laws and
19 regulations;
- 20

- 1 d. if Defendant's data security systems prior to and during the Data
2 Breach were consistent with industry standards;
- 3 e. if Defendant owed a duty to Class Members to safeguard their
4 PII;
- 5 f. if Defendant breached their duty to Class Members to safeguard
6 their PII;
- 7 g. if Defendant knew or should have known that their data security
8 systems and monitoring processes were deficient;
- 9 h. if Defendant should have discovered the Data Breach sooner;
- 10 i. if Plaintiff and Class Members suffered legally cognizable
11 damages as a result of Defendant's misconduct;
- 12 j. if Defendant's conduct was negligent;
- 13 k. if Defendant's breach implied contracts with Plaintiff and Class
14 Members;
- 15 l. if Defendant were unjustly enriched by unlawfully retaining a
16 benefit conferred upon them by Plaintiff and Class Members;
- 17 m. if Defendant failed to provide notice of the Data Breach in a
18 timely manner, and;
- 19
20
21

1 litigation. Absent a class action, most Class Members would likely find that the cost
2 of litigating their individual claims is prohibitively high and would therefore have
3 no effective remedy. The prosecution of separate actions by individual Class
4 Members would create a risk of inconsistent or varying adjudications with respect
5 to individual Class Members, which would establish incompatible standards of
6 conduct for Defendant. In contrast, the conduct of this action as a Class action
7 presents far fewer management difficulties, conserves judicial resources and the
8 parties' resources, and protects the rights of each Class Member.

9 118. Defendant has acted on grounds that apply generally to the Class as a
10 whole, so that Class certification, injunctive relief, and corresponding declaratory
11 relief are appropriate on a Class-wide basis.

12 119. Likewise, particular issues under Rule 42(d)(1) are appropriate for
13 certification because such claims present only particular, common issues, the
14 resolution of which would advance the disposition of this matter and the parties'
15 interests therein. Such particular issues include, but are not limited to:

- 16 a. if Defendant failed to timely notify the public of the Data
17 Breach;

- 1 b. if Defendant owed a legal duty to Plaintiff and the Class to
2 exercise due care in collecting, storing, and safeguarding their
3 PII;
- 4 c. if Defendant’s security measures to protect their data systems
5 were reasonable in light of best practices recommended by data
6 security experts;
- 7 d. if Defendant’s failure to institute adequate protective security
8 measures amounted to negligence;
- 9 e. if Defendant failed to take commercially reasonable steps to
10 safeguard consumer PII; and
- 11 f. if adherence to FTC data security recommendations, and
12 measures recommended by data security experts would have
13 reasonably prevented the Data Breach.

14 120. Finally, all members of the proposed Class are readily ascertainable.
15 Defendant has access to Class Members' names and addresses affected by the Data
16 Breach. Class Members have already been preliminarily identified and sent notice
17 of the Data Breach by Defendant.

18 **FIRST CAUSE OF ACTION**
19 **Negligence**
20 **(On Behalf of Plaintiff and the Class)**

1 121. Plaintiff repeats and re-alleges paragraphs 1 through 119 of this
2 Complaint and incorporates them by reference herein.

3 122. Plaintiff and the Class entrusted Defendant with their PII on the
4 premise and with the understanding that Defendant would safeguard their
5 information, use their PII for business purposes only, and/or not disclose their PII
6 to unauthorized third parties.

7 123. Defendant has full knowledge of the sensitivity of the PII and the types
8 of harm that Plaintiff and the Class could and would suffer if the PII were
9 wrongfully disclosed.

10 124. By collecting and storing this data in their computer system and
11 network, and sharing it and using it for commercial gain, Defendant owed a duty of
12 care to use reasonable means to secure and safeguard their computer system—and
13 Class Members' PII held within it—to prevent disclosure of the information, and
14 to safeguard the information from theft. Defendant's duty included a responsibility
15 to implement processes by which it could detect a breach of their security systems
16 in a reasonably expeditious period of time and to give prompt notice to those
17 affected in the case of a data breach.

18 125. Defendant owed a duty of care to Plaintiff and Class Members to
19 provide data security consistent with industry standards and other requirements
20

1 discussed herein, and to ensure that their systems and networks, and the personnel
2 responsible for them, adequately protected the PII.

3 126. Defendant’s duty of care to use reasonable security measures arose as
4 a result of the special relationship that existed between Defendant and individuals
5 who entrusted them with PII, which is recognized by laws and regulations, as well
6 as common law. Defendant was in a superior position to ensure that their systems
7 were sufficient to protect against the foreseeable risk of harm to Class Members
8 from a data breach.

9 127. Defendant’s duty to use reasonable security measures required
10 Defendant to reasonably protect confidential data from any intentional or
11 unintentional use or disclosure.

12 128. In addition, Defendant had a duty to employ reasonable security
13 measures under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45,
14 which prohibits “unfair . . . practices in or affecting commerce,” including, as
15 interpreted and enforced by the FTC, the unfair practice of failing to use reasonable
16 measures to protect confidential data.

17 129. Defendant’s duty to use reasonable care in protecting confidential data
18 arose not only as a result of the statutes and regulations described above, but also
19 because Defendant are bound by industry standards to protect confidential PII.
20

1 necessary for Plaintiff and Class Members to take appropriate measures to protect
2 their PII, to be vigilant in the face of an increased risk of harm, and to take other
3 necessary steps to mitigate the harm caused by the data breach.

4 132. Plaintiff and Class Members are also entitled to injunctive relief
5 requiring Defendant to, *e.g.*, (i) strengthen their data security systems and
6 monitoring procedures; (ii) submit to future annual audits of those systems and
7 monitoring procedures; and (iii) continue to provide adequate credit monitoring to
8 all Class Members.

9 133. Defendant breached its duties to Plaintiff and Class Members by
10 failing to provide fair, reasonable, or adequate computer systems and data security
11 practices to safeguard Plaintiff's and Class Members' PII.

12 134. Defendant owed these duties to Plaintiff and Class Members because
13 they are members of a well-defined, foreseeable, and probable class of individuals
14 whom Defendant knew or should have known would suffer injury-in-fact from
15 Defendant's inadequate security protocols. Defendant actively sought and obtained
16 Plaintiff's and Class Members' PII.

17 135. The risk that unauthorized persons would attempt to gain access to
18 the PII and misuse it was foreseeable. Given that Defendant holds vast amounts
19 of PII, it was inevitable that unauthorized individuals would attempt to access
20

1 Defendant's databases containing the PII—whether by malware or otherwise.

2 136. PII is highly valuable, and Defendant knew, or should have known, the
3 risk in obtaining, using, handling, emailing, and storing the PII of Plaintiff and
4 Class Members and the importance of exercising reasonable care in handling it.

5 137. Defendant breached its duties by failing to exercise reasonable care in
6 supervising their agents, contractors, vendors, and suppliers, and in handling
7 and securing the PII of Plaintiff and Class Members—which actually and
8 proximately caused the Data Breach and injured Plaintiff and Class Members.

9 138. Defendant further breached its duties by failing to provide reasonably
10 timely notice of the data breach to Plaintiff and Class Members, which actually
11 and proximately caused and exacerbated the harm from the data breach and
12 Plaintiff and Class Members' injuries-in-fact. As a direct and traceable result of
13 Defendant's negligence and/or negligent supervision, Plaintiff and Class Members
14 have suffered or will suffer damages, including monetary damages, increased risk
15 of future harm, embarrassment, humiliation, frustration, and emotional distress.

16 139. Defendant's breach of its common-law duties to exercise reasonable
17 care and their failures and negligence actually and proximately caused Plaintiff
18 and Class Members actual, tangible, injury-in-fact and damages, including,
19 without limitation, the theft of their PII by criminals, improper disclosure of
20

1 their PII, lost benefit of their bargain, lost value of their PII, and lost time and
2 money incurred to mitigate and remediate the effects of the data breach that
3 resulted from and were caused by Defendant's negligence, which injury-in-fact
4 and damages are ongoing, imminent, immediate, and which they continue to face.

5 **SECOND CAUSE OF ACTION**

6 ***Negligence per se***

7 **(On behalf of the Plaintiff and the Class)**

8 140. Plaintiff repeats and re-alleges paragraphs 1 through 119 of this
9 Complaint and incorporates them by reference herein.

10 141. Pursuant to the Federal Trade Commission Act, 15 U.S.C. § 45,
11 Defendant had a duty to provide fair and adequate computer systems and data
12 security practices to safeguard Plaintiff's and Class members' Private Information.

13 142. Defendant breached its duties to Plaintiff and Class members under
14 the FTC Act by failing to provide fair, reasonable, or adequate computer systems
15 and data security practices to safeguard Plaintiff's and Class members' Private
16 Information.

17 143. Defendant's failure to comply with applicable laws and regulations
18 constitutes negligence *per se*.

19 144. The injuries to Plaintiff and Class members resulting from the Data
20 Breach were directly and indirectly caused by Defendant's violation of the statutes

1 described herein.

2 145. Plaintiff and Class members were within the class of persons the
3 Federal Trade Commission Act intended to protect and the type of harm that
4 resulted from the Data Breach was the type of harm these statutes were intended to
5 guard against.

6 146. But for Defendant's wrongful and negligent breach of its duties owed
7 to Plaintiff and Class members, Plaintiff and Class members would not have been
8 injured.

9 147. The injuries and harms suffered by Plaintiff and Class members were
10 the reasonably foreseeable result of Defendant's breach of its duties. Defendant
11 knew or should have known that it was failing to meet its duties and that
12 Defendant's breach would cause Plaintiff and Class members to experience the
13 foreseeable harms associated with the exposure of their Private Information.

14 148. As a direct and proximate result of Defendant's negligent conduct,
15 Plaintiff and Class members have suffered injuries and are entitled to
16 compensatory, consequential, and punitive damages in an amount to be proven at
17 trial.

18 **THIRD CAUSE OF ACTION**
19 **Breach of Implied Contract**
20 **(On behalf of the Plaintiff and the Class)**

1 153. Plaintiff and the Class would not have entrusted their PII to Defendant
2 had they known that Defendant would make the PII internet-accessible, not encrypt
3 sensitive data elements, and not delete the PII that Defendant no longer had a
4 reasonable need to maintain it.

5 154. Plaintiff and the Class fully performed their obligations under the
6 implied contracts with Defendant.

7 155. Defendant breached the implied contracts they made with Plaintiff and
8 the Class by failing to safeguard and protect their personal information, by failing
9 to delete the information of Plaintiff and the Class once the relationship ended, and
10 by failing to provide timely and accurate notice to them that personal information
11 was compromised as a result of the Data Breach.

12 156. As a direct and proximate result of Defendant's above-described
13 breach of implied contract, Plaintiff and the Class have suffered (and will continue
14 to suffer) ongoing, imminent, and impending threat of identity theft crimes, fraud,
15 and abuse, resulting in monetary loss and economic harm; actual identity theft
16 crimes, fraud, and abuse, resulting in monetary loss and economic harm; loss of the
17 confidentiality of the stolen confidential data; the illegal sale of the compromised
18 data on the dark web; expenses and/or time spent on credit monitoring and identity
19 theft insurance; time spent scrutinizing bank statements, credit card statements, and
20

1 credit reports; expenses and/or time spent initiating fraud alerts, decreased credit
2 scores and ratings; lost work time; and other economic and non-economic harm.

3 157. As a direct and proximate result of Defendant's above-described
4 breach of implied contract, Plaintiff and the Class are entitled to recover actual,
5 consequential, and nominal damages to be determined at trial.

6 **FOURTH CAUSE OF ACTION**

7 **Invasion of Privacy**

8 **(On behalf of the Plaintiff and the Class)**

9 158. Plaintiff repeats and re-alleges paragraphs 1 through 119 of this
10 Complaint and incorporates them by reference herein.

11 159. Plaintiff and Class Members had a legitimate expectation of privacy
12 regarding their PII and were accordingly entitled to the protection of this
13 information against disclosure to unauthorized third parties.

14 160. Defendant owed a duty to Plaintiff and Class Member to keep their PII
15 confidential.

16 161. The unauthorized disclosure and/or acquisition (*i.e.*, theft) by a third
17 party of Plaintiff's and Class Members' PII is highly offensive to a reasonable
18 person.

19 162. Defendant's reckless and negligent failure to protect Plaintiff's and
20 Class Members' PII constitutes an intentional interference with Plaintiff's and the
21

1 Class Members' interest in solitude or seclusion, either as to their person or as to
2 their private affairs or concerns, of a kind that would be highly offensive to a
3 reasonable person.

4 163. Defendant's failure to protect Plaintiff's and Class Members' PII acted
5 with a knowing state of mind when it permitted the Data Breach because it knew
6 its information security practices were inadequate.

7 164. Defendant knowingly did not notify Plaintiff and Class Members in a
8 timely fashion about the Data Breach.

9 165. Because Defendant failed to properly safeguard Plaintiff's and Class
10 Members' PII, Defendant had notice and knew that its inadequate cybersecurity
11 practices would cause injury to Plaintiff and the Class.

12 166. As a proximate result of Defendant's acts and omissions, the private
13 and sensitive PII of Plaintiff and the Class Members was stolen by a third party and
14 is now available for disclosure and redisclosure without authorization, causing
15 Plaintiff and the Class to suffer damages.

16 167. Defendant's wrongful conduct will continue to cause great and
17 irreparable injury to Plaintiff and the Class since their PII is still maintained by
18 Defendant with their inadequate cybersecurity system and policies.

1 168. Plaintiff and Class Members have no adequate remedy at law for the
2 injuries relating to Defendant's continued possession of their sensitive and
3 confidential records. A judgment for monetary damages will not end Defendant's
4 inability to safeguard the PII of Plaintiff and the Class.

5 169. Plaintiff, on behalf of themselves and Class Members, seeks injunctive
6 relief to enjoin Defendant from further intruding into the privacy and confidentiality
7 of Plaintiff's and Class Members' PII.

8 170. Plaintiff, on behalf of themselves and Class Members, seeks
9 compensatory damages for Defendant's invasion of privacy, which includes the
10 value of the privacy interest invaded by Defendant, the costs of future monitoring
11 of their credit history for identity theft and fraud, plus prejudgment interest, and
12 costs.

13 //

14 //

15 **FIFTH CAUSE OF ACTION**
16 **Breach of Fiduciary Duty**
(On Behalf of Plaintiff and the Class)

17 171. Plaintiff repeats and re-alleges paragraphs 1 through 119 of this
18 Complaint and incorporates them by reference herein.

19 172. In providing their PII, directly or indirectly, to Defendant, Plaintiffs
20 and Class members justifiably placed a special confidence in Defendant to act in

1 good faith and with due regard to interests of Plaintiffs and class members to
2 safeguard and keep confidential that PII.

3 173. Defendant accepted the special confidence Plaintiffs and Class
4 members placed in it, as evidenced by its assertion that it is committed to protecting
5 the privacy of Plaintiffs' and Class Members' personal information as detailed in
6 its Privacy Policy.

7 174. In light of the special relationship between Defendant and Plaintiffs
8 and Class members, whereby Defendant became a guardian of Plaintiffs' and Class
9 members' PII, Defendant became a fiduciary by its undertaking and guardianship
10 of the PII, to act primarily for the benefit of its customers, including Plaintiff and
11 Class members, for the safeguarding of Plaintiffs' and Class members' PII.

12 175. Defendant has a fiduciary duty to act for the benefit of Plaintiffs and
13 Class members upon matters within the scope of its relationship with Defendants'
14 customers, in particular, to keep secure the PII of its customers.

15 176. Defendant breached its fiduciary duties to Plaintiffs and Class
16 members by failing to protect the integrity of the systems containing Plaintiffs' and
17 Class members' PII.

18 177. Defendant breached its fiduciary duties to Plaintiffs and class
19 members by otherwise failing to safeguard Plaintiffs' and Class members' PII.
20

1 178. As a direct and proximate result of Defendant's breaches of its
2 fiduciary duties, Plaintiffs and class members have suffered and will suffer injury,
3 including but not limited to: (i) invasion of privacy; (ii) lost or diminished value of
4 PII; (iii) lost time and opportunity costs associated with attempting to mitigate the
5 actual consequences of the Data Breach; (iv) loss of benefit of the bargain; and (v)
6 the continued and certainly increased risk to their PII, which: (a) remains
7 unencrypted and available for unauthorized third parties to access and abuse; and
8 (b) remains backed up in Defendant's possession and is subject to further
9 unauthorized disclosures so long as Defendant fails to undertake appropriate and
10 adequate measures to protect the PII.

11 179. As a direct and proximate result of Defendant's breaches of its
12 fiduciary duties, Plaintiffs and Class members have suffered and will continue to
13 suffer other forms of injury and/or harm, and other economic and non-economic
14 losses.

15 **SIXTH CAUSE OF ACTION**

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

18 180. Plaintiff repeats and re-alleges paragraphs 1 through 119 of this
19 Complaint and incorporates them by reference herein.

20 181. Defendant violated Cal. Bus. and Prof. Code § 17200, et seq., by

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

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

13 183. In addition, Defendant engaged in unlawful acts and practices by
14 failing to disclose the Data Breach in a timely and accurate manner, contrary to the
15 duties imposed by Cal. Civ. Code § 1798.82.

16 184. As a direct and proximate result of Defendant’s unlawful practices and
17 acts, Plaintiff and Class Members were injured and lost money or property,
18 including but not limited to the price received by Defendant for the products and
19 services, the loss of Plaintiff’s and Class Members’ legally protected interest in the
20

1 confidentiality and privacy of their PII, nominal damages, and additional losses as
2 described herein.

3 185. Defendant knew or should have known that its computer systems and
4 data security practices were inadequate to safeguard Plaintiff's and Class Members'
5 PII and that the risk of a data breach or theft was highly likely. Defendant's actions
6 in engaging in the above-named unlawful practices and acts were negligent,
7 knowing and willful, and/or wanton and reckless with respect to the rights of
8 Plaintiff and Class Members.

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

16 **SEVENTH CAUSE OF ACTION**
17 **Violations of the California Consumer Privacy Act ("CCPA")**
18 **Cal. Civ. Code § 1798.150**
19 **(On Behalf of Plaintiff and the Class)**

20 187. Plaintiff repeats and realleges paragraphs 1 through 119 of this
21 Complaint and incorporates them by reference herein.

1 188. Defendant violated California Civil Code § 1798.150 of the CCPA by
2 failing to implement and maintain reasonable security procedures and practices
3 appropriate to the nature of the information to protect the nonencrypted PII of
4 Plaintiffs and the California Subclass. As a direct and proximate result, Plaintiffs
5 and the California Subclass’s nonencrypted and nonredacted PII was subject to
6 unauthorized access and exfiltration, theft, or disclosure.

7 189. Defendant is a “business” under the meaning of Civil Code § 1798.140
8 because Defendant is a “corporation, association, or other legal entity that is
9 organized or operated for the profit or financial benefit of its shareholders or other
10 owners” that “collects consumers’ personal information” and is active “in the State
11 of California” and “had annual gross revenues in excess of twenty-five million
12 dollars (\$25,000,000) in the preceding calendar year.” Civil Code § 1798.140(d).

13 190. Plaintiff and Class Members seek injunctive or other equitable relief
14 to ensure Defendant hereinafter adequately safeguards PII by implementing
15 reasonable security procedures and practices. Such relief is particularly important
16 because Defendant continues to hold PII, including Plaintiffs and California
17 Subclass members’ PII. Plaintiff and Class members have an interest in ensuring
18 that their PII is reasonably protected, and Defendant has demonstrated a pattern of
19 failing to adequately safeguard this information.
20

1 191. Pursuant to California Civil Code § 1798.150(b), Plaintiff mailed a
2 CCPA notice letter to Defendant’s registered service agents, detailing the specific
3 provisions of the CCPA that Defendant has violated and continues to violate. If
4 Defendant cannot cure within 30 days—and Plaintiff believes such cure is not
5 possible under these facts and circumstances—then Plaintiff intends to promptly
6 amend this Complaint to seek statutory damages as permitted by the CCPA.

7 192. As described herein, an actual controversy has arisen and now exists
8 as to whether Defendant implemented and maintained reasonable security
9 procedures and practices appropriate to the nature of the information so as to protect
10 the personal information under the CCPA.

11 193. A judicial determination of this issue is necessary and appropriate at
12 this time under the circumstances to prevent further data breaches by Defendant.

13 //

14 //

15 **EIGHTH CAUSE OF ACTION**
16 **Violations of the California Consumer Records Act**
17 **Cal. Civ. Code § 1798.80, *et seq.***
 (On Behalf of Plaintiff and the Class)

18 194. Plaintiff repeats and re-alleges paragraphs 1 through 119 of this
19 Complaint and incorporates them by reference herein.

20 195. Under the California Consumer Records Act, any “person or business

1 that conducts business in California, and that owns or licenses computerized data
2 that includes personal information” must “disclose any breach of the system
3 following discovery or notification of the breach in the security of the data to any
4 resident of California whose unencrypted personal information was, or is
5 reasonably believes to have been, acquired by an unauthorized person.” Cal. Civ.
6 Code § 1798.82. The disclosure must “be made in the most expedient time possible
7 and without unreasonable delay” but disclosure must occur “immediately following
8 discovery [of the breach], if the personal information was, or is reasonable believes
9 to have been, acquired by an unauthorized person.” *Id.* (emphasis added).

10 196. The Data Breach constitutes a “breach of the security system” of
11 Defendant.

12 197. An unauthorized person acquired the personal, unencrypted
13 information of Plaintiff and the Class.

14 198. Defendant knew that an unauthorized person had acquired the
15 personal, unencrypted information of Plaintiff and the Class but waited almost
16 eleven months to notify them. Given the severity of the Data Breach, this is an
17 unreasonable delay.

18 199. Defendant’s unreasonable delay prevent Plaintiff and the Class from
19 taking appropriate measures from protecting themselves against harm.

1 B. For equitable relief enjoining Defendant from engaging in the
2 wrongful conduct complained of herein pertaining to the misuse
3 and/or disclosure of the PII of Plaintiff and Class Members;

4 C. For injunctive relief requested by Plaintiff, including but not limited
5 to, injunctive and other equitable relief as is necessary to protect the
6 interests of Plaintiff and Class Members, including but not limited to
7 an order;

8 i. prohibiting Defendant from engaging in the wrongful and
9 unlawful acts described herein;

10 ii. requiring Defendant to protect, including through
11 encryption, all data collected through the course of its
12 business in accordance with all applicable regulations,
13 industry standards, and federal, state or local laws;

14 iii. requiring Defendant to delete, destroy, and purge the
15 personal identifying information of Plaintiff and Class
16 Members unless Defendant can provide to the Court
17 reasonable justification for the retention and use of such
18 information when weighed against the privacy interests
19 of Plaintiff and Class Members;

1 security auditors and internal personnel to run automated
2 security monitoring;

3 ix. requiring Defendant to audit, test, and train its security
4 personnel regarding any new or modified procedures;

5 x. requiring Defendant to segment data by, among other
6 things, creating firewalls and access controls so that if
7 one area of Defendant's network is compromised,
8 hackers cannot gain access to other portions of
9 Defendant's systems;

10 xi. requiring Defendant to conduct regular database scanning
11 and securing checks;

12 xii. requiring Defendant to establish an information security
13 training program that includes at least annual information
14 security training for all employees, with additional
15 training to be provided as appropriate based upon the
16 employees' respective responsibilities with handling
17 personal identifying information, as well as protecting the
18 personal identifying information of Plaintiff and Class
19 Members;

1 Members about the threats that they face as a result of the
2 loss of their confidential personal identifying information
3 to third parties, as well as the steps affected individuals
4 must take to protect themselves; and

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

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

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

1 F. For prejudgment and post-judgement interest on all amounts awarded;

2 G. Granting Plaintiff and the Class leave to amend this Complaint to
3 conform to the evidence produced at trial; and

4 H. Such other and further relief as this Court may deem just and proper.

5 **JURY TRIAL DEMANDED**

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

7 Dated: May 8, 2024

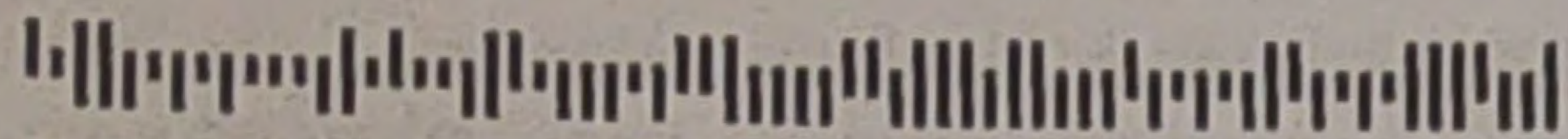
Respectfully Submitted,

8
9 By: /s/ Scott Edelsberg
10 Scott Edelsberg (CA Bar No. 330990)
11 **EDELSBERG LAW, P.A.**
12 1925 Century Park E #1700
13 Los Angeles, CA 90067
14 Tel: (305) 975-3320
15 Email: scott@edelsberglaw.com

16
17
18
19
20
21 *Attorney for Plaintiff and Proposed Class*

EXHIBIT A

NOTICE OF DATA BREACH



DANIEL JIMENEZ JR



April 30, 2024

Dear Daniel Jimenez Jr:

The privacy and security of the personal information we maintain is of the utmost importance to OE Federal Credit Union ("OEFUCU"). We are writing with important information regarding a recent security incident that may have impacted some of your information. We want to provide you with information about the incident, tell you about the services that we are providing to you, and let you know that we continue to take significant measures to protect your information.

What Happened?

On or about October 28, 2023, OEFUCU detected unauthorized access to our network as a result of a cybersecurity incident that resulted in the potential exposure of the data we maintain.

What We Are Doing.

Upon learning of this issue, we immediately began efforts to secure our network and commenced a prompt and thorough investigation. As part of our investigation, we have been working very closely with external cybersecurity professionals experienced in handling these types of incidents. After an extensive forensic investigation and document review, we discovered on April 1, 2024, that between approximately August 19, 2023 and October 29, 2023, certain impacted files containing personal information may have been accessed and/or acquired by an unauthorized party.

What Information Was Involved?

The impacted information includes your full name, and Social Security number, driver's license or government ID number.

What You Can Do.

We have no evidence that any of your information has been used for identity theft or financial fraud as a result of this incident. Nevertheless, out of an abundance of caution, we want to make you aware of the incident. To protect you from potential misuse of your information, we are providing you with access to a complimentary 12-month membership of Experian IdentityWorksSM. For more information on identity theft prevention and IdentityWorks Credit 3B, including instructions on how to activate your complimentary 12-month membership, please see the additional information provided in this letter.

ClassAction.org

This complaint is part of ClassAction.org's searchable class action lawsuit database and can be found in this post: [OE Federal Credit Union Hit with Class Action Lawsuit Over 2023 Data Breach](#)
