

1 Scott Edward Cole, Esq. (S.B. #160744)
Laura Grace Van Note, Esq. (S.B. #310160)
2 **COLE & VAN NOTE**
555 12th Street, Suite 2100
3 Oakland, California 94607
Telephone: (510) 891-9800
4 Facsimile: (510) 891-7030
Email: sec@colevannote.com
5 Email: lvn@colevannote.com

6 Attorneys for Representative Plaintiff
and the Plaintiff Class

7
8 **UNITED STATES DISTRICT COURT**
9 **NORTHERN DISTRICT OF CALIFORNIA**
10

11 EILEEN POLUK, individually, and on
behalf of all others similarly situated,

12 Plaintiff,

14 v.

15 PATELCO CREDIT UNION,

16 Defendant.

Case No.

CLASS ACTION

COMPLAINT FOR DAMAGES

[JURY TRIAL DEMANDED]

17
18
19 **INTRODUCTION**

20 1. Representative Plaintiff Eileen Poluk (“Representative Plaintiff”) brings this class
21 action against Defendant Patelco Credit Union (“Defendant”) for its failure to properly secure and
22 safeguard Representative Plaintiff’s and/or Class Members’ personally identifiable information
23 stored within Defendant’s information network (these types of information, *inter alia*, being
24 thereafter referred to, collectively, as “personally identifiable information” or “PII”).¹ All such
25 information is referred to in the aggregate herein as “Private Information.”

26
27 ¹ Personally identifiable information (“PII”) generally incorporates information that can be
28 used to distinguish or trace an individual’s identity, either alone or when combined with other
personal or identifying information. 2 C.F.R. § 200.79. At a minimum, it includes all information
that on its face expressly identifies an individual. PII also is generally defined to include certain

COLE & VAN NOTE
ATTORNEYS AT LAW
555 12TH STREET, SUITE 2100
OAKLAND, CA 94607
TEL: (510) 891-9800

COLE & VAN NOTE
ATTORNEYS AT LAW
555 12TH STREET, SUITE 2100
OAKLAND, CA 94607
TEL: (510) 891-9800

1 2. With this action, Representative Plaintiff seeks to hold Defendant responsible for
2 the harms it caused and will continue to cause Representative Plaintiff and other similarly situated
3 persons in the massive and preventable cyberattack purportedly discovered by Defendant on June
4 29, 2024, by which cybercriminals infiltrated Defendant’s inadequately protected network and
5 accessed the Private Information which was being kept under-protected (the “Data Breach”).

6 3. While Defendant claims to have discovered the breach as early as June 29, 2024,
7 Defendant did not begin informing victims of the Data Breach until June 30, 2024, and failed to
8 inform victims when or for how long the Data Breach occurred. Indeed, Representative Plaintiff
9 and Class Members were wholly unaware of the Data Breach until they received letters from
10 Defendant informing them of it.

11 4. Defendant acquired, collected and stored Representative Plaintiff’s and Class
12 Members’ Private Information. Therefore, at all relevant times, Defendant knew or should have
13 known that Representative Plaintiff and Class Members would use Defendant’s services to store
14 and/or share sensitive data, including highly confidential Private Information.

15 5. Defendant disregarded the rights of Representative Plaintiff and Class Members by
16 intentionally, willfully, recklessly and/or negligently failing to take and implement adequate and
17 reasonable measures to ensure that Representative Plaintiff’s and Class Members’ Private
18 Information was safeguarded, failing to take available steps to prevent an unauthorized disclosure
19 of data, and failing to follow applicable, required and appropriate protocols, policies and
20 procedures regarding the encryption of data, even for internal use. As a result, Representative
21 Plaintiff’s and Class Members’ Private Information was compromised through disclosure to an
22 unknown and unauthorized third party—an undoubtedly nefarious third party seeking to profit off
23 this disclosure by defrauding Representative Plaintiff and Class Members in the future.
24 Representative Plaintiff and Class Members have a continuing interest in ensuring their
25 information is and remains safe and are entitled to injunctive and other equitable relief.

26
27 _____
28 identifiers that do not on its face name an individual, but that are considered to be particularly
sensitive and/or valuable if in the wrong hands (for example, Social Security numbers, passport
numbers, driver’s license numbers, financial account numbers, etc.).

JURISDICTION AND VENUE

1
2 6. Jurisdiction is proper in this Court under 28 U.S.C. § 1332 (diversity jurisdiction).
3 Specifically, this Court has subject matter and diversity jurisdiction over this action under 28
4 U.S.C. § 1332(d) because this is a class action where the amount in controversy exceeds the sum
5 or value of \$5 million, exclusive of interest and costs, there are more than 100 members in the
6 proposed class and at least one other Class Member is a citizen of a state different from Defendant.

7 7. Supplemental jurisdiction to adjudicate issues pertaining to state law is proper in
8 this Court under 28 U.S.C. § 1367.

9 8. Defendant is headquartered and routinely conducts business in the State where this
10 District is located, has sufficient minimum contacts in this State and has intentionally availed itself
11 of this jurisdiction by marketing and selling products and services, and by accepting and processing
12 payments for those products and services within this State.

13 9. Venue is proper in this Court under 28 U.S.C. § 1391 because a substantial part of
14 the events that gave rise to Representative Plaintiff's claims took place within this District, and
15 Defendant does business in this Judicial District.

16
17 **PLAINTIFF**

18 10. Representative Plaintiff is an adult individual and, at all relevant times herein, was
19 a resident and citizen of the State of California. Representative Plaintiff is a victim of the Data
20 Breach.

21 11. Defendant received highly sensitive Private Information from Representative
22 Plaintiff in connection with the services Representative Plaintiff obtained. As a result,
23 Representative Plaintiff's information was among the data accessed by an unauthorized third party
24 in the Data Breach.

25 12. At all times herein relevant, Representative Plaintiff is and was a member of the
26 Class.

COLE & VAN NOTE
ATTORNEYS AT LAW
555 12TH STREET, SUITE 2100
OAKLAND, CA 94607
TEL: (510) 891-9800

COLE & VAN NOTE
ATTORNEYS AT LAW
555 12TH STREET, SUITE 2100
OAKLAND, CA 94607
TEL: (510) 891-9800

1 13. Representative Plaintiff’s Private Information was exposed in the Data Breach
2 because Defendant stored and/or shared Representative Plaintiff’s Private Information.
3 Representative Plaintiff’s Private Information was within the possession and control of Defendant
4 at the time of the Data Breach.

5 14. Representative Plaintiff received a letter from Defendant stating Representative
6 Plaintiff’s Private Information was involved in the Data Breach (the “Notice”).

7 15. As a result, Representative Plaintiff spent time dealing with the consequences of
8 the Data Breach, which included and continues to include, time spent verifying the legitimacy and
9 impact of the Data Breach, exploring credit monitoring and identity theft insurance options, self-
10 monitoring Representative Plaintiff’s accounts and seeking legal counsel regarding Representative
11 Plaintiff’s options for remedying and/or mitigating the effects of the Data Breach. This time has
12 been lost forever and cannot be recaptured.

13 16. Representative Plaintiff suffered actual injury in the form of damages to and
14 diminution in the value of Representative Plaintiff’s Private Information—a form of intangible
15 property that Representative Plaintiff entrusted to Defendant, which was compromised in and as a
16 result of the Data Breach.

17 17. Representative Plaintiff suffered lost time, annoyance, interference and
18 inconvenience as a result of the Data Breach and has anxiety and increased concerns for the loss
19 of privacy, as well as anxiety over the impact of cybercriminals accessing, using and selling
20 Representative Plaintiff’s Private Information.

21 18. Representative Plaintiff suffered imminent and impending injury arising from the
22 substantially increased risk of fraud, identity theft and misuse resulting from Representative
23 Plaintiff’s Private Information being placed in the hands of unauthorized third parties/criminals.
24 Representative Plaintiff has a continuing interest in ensuring that Representative Plaintiff’s Private
25 Information, which, upon information and belief, remains backed up in Defendant’s possession, is
26 protected and safeguarded from future breaches.

27
28

1 **DEFENDANT**

2 19. Defendant is a non-profit corporation with a principal place of business located in
3 Dublin, California. Defendant is the 22nd largest credit union serving Northern California,
4 particularly the San Francisco Bay Area.²

5 20. The true names and capacities of persons or entities, whether individual, corporate,
6 associate or otherwise, who may be responsible for some of the claims alleged here are currently
7 unknown to Representative Plaintiff. Representative Plaintiff will seek leave of court to amend
8 this Complaint to reflect the true names and capacities of such responsible parties when their
9 identities become known.

10
11 **CLASS ACTION ALLEGATIONS**

12 21. Representative Plaintiff brings this action pursuant to the provisions of Rules 23(a),
13 (b)(2), and (b)(3) of the Federal Rules of Civil Procedure, on behalf of Representative Plaintiff and
14 the following class (collectively, the “Class”):

15 **Nationwide Class:**

16 “All individuals within the United States of America whose Private
17 Information was exposed to unauthorized third parties as a result of the data
18 breach allegedly discovered by Defendant on or before June 29, 2024.”

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

26 23. In the alternative, Representative Plaintiff may request additional subclasses as
27 necessary based, e.g., on the types of Private Information that were compromised.

28 ² <https://www.patelco.org/about-patelco/who-we-are/> (last accessed, July 1, 2024).

COLE & VAN NOTE
 ATTORNEYS AT LAW
 555 12TH STREET, SUITE 2100
 OAKLAND, CA 94607
 TEL: (510) 891-9800

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

24. Representative Plaintiff reserves the right to amend the above definition or to propose subclasses in subsequent pleadings and its motion for class certification.

25. This action has been brought and may properly be maintained as a class action under Federal Rules of Civil Procedure Rule 23 because there is a well-defined community of interest in the litigation and membership in the proposed Classes is easily ascertainable.

a. Numerosity: A class action is the only available method for the fair and efficient adjudication of this controversy. The members of the Plaintiff Classes are so numerous that joinder of all members is impractical, if not impossible. Membership in the Class(es) will be determined by analysis of Defendant’s records.

b. Commonality: Representative Plaintiff and Class Members share a community of interest in that there are numerous common questions and issues of fact and law which predominate over any questions and issues solely affecting individual members, including, but not necessarily limited to:

- 1) Whether Defendant had a legal duty to Representative Plaintiff and the Classes to exercise due care in collecting, storing, using and/or safeguarding their Private Information;
- 2) Whether Defendant knew or should have known of the susceptibility of its data security systems to a data breach;
- 3) Whether Defendant’s security procedures and practices to protect its systems were reasonable in light of the measures recommended by data security experts;
- 4) Whether Defendant’s failure to implement adequate data security measures allowed the Data Breach to occur;
- 5) Whether Defendant failed to comply with its own policies and applicable laws, regulations and industry standards relating to data security;
- 6) Whether Defendant adequately, promptly and accurately informed Representative Plaintiff and Class Members that their Private Information had been compromised;
- 7) How and when Defendant actually learned of the Data Breach;
- 8) Whether Defendant’s conduct, including its failure to act, resulted in or was the proximate cause of the breach of its systems, resulting in the loss of Representative Plaintiff’s and Class Members’ Private Information;
- 9) Whether Defendant adequately addressed and fixed the vulnerabilities which permitted the Data Breach to occur;

COLE & VAN NOTE
ATTORNEYS AT LAW
555 12TH STREET, SUITE 2100
OAKLAND, CA 94607
TEL: (510) 891-9800

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

- 10) Whether Defendant engaged in unfair, unlawful or deceptive practices by failing to safeguard Representative Plaintiff's and Class Members' Private Information;
- 11) Whether Representative Plaintiff and Class Members are entitled to actual and/or statutory damages and/or whether injunctive, corrective and/or declaratory relief and/or an accounting is/are appropriate as a result of Defendant's wrongful conduct; and
- 12) Whether Representative Plaintiff and Class Members are entitled to restitution as a result of Defendant's wrongful conduct.

c. Typicality: Representative Plaintiff's claims are typical of the claims of the Plaintiff Classes. Representative Plaintiff and all members of the Plaintiff Classes sustained damages arising out of and caused by Defendant's common course of conduct in violation of law, as alleged herein.

d. Adequacy of Representation: Representative Plaintiff in this class action is an adequate representative of each of the Plaintiff Classes in that the Representative Plaintiff has the same interest in the litigation of this case as the Class Members, is committed to vigorous prosecution of this case and has retained competent counsel who are experienced in conducting litigation of this nature. Representative Plaintiff is not subject to any individual defenses unique from those conceivably applicable to other Class Members or the Classes in their entirety. Representative Plaintiff anticipates no management difficulties in this litigation.

e. Superiority of Class Action: Since the damages suffered by individual Class Members, while not inconsequential, may be relatively small, the expense and burden of individual litigation by each member makes or may make it impractical for members of the Plaintiff Classes to seek redress individually for the wrongful conduct alleged herein. Should separate actions be brought or be required to be brought by each individual member of the Plaintiff Classes, the resulting multiplicity of lawsuits would cause undue hardship and expense for the Court and the litigants. The prosecution of separate actions would also create a risk of inconsistent rulings which might be dispositive of the interests of the Class Members who are not parties to the adjudications and/or may substantially impede their ability to adequately protect their interests.

26. Class certification is proper because the questions raised by this Complaint are of common or general interest affecting numerous persons, such that it is impracticable to bring all Class Members before the Court.

27. This class action is also appropriate for certification because Defendant has acted or refused to act on grounds generally applicable to Class Members, thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward the Class Members and making final injunctive relief appropriate with respect to the Classes in their entirety.

COLE & VAN NOTE
ATTORNEYS AT LAW
555 12TH STREET, SUITE 2100
OAKLAND, CA 94607
TEL: (510) 891-9800

1 Defendant’s policies and practices challenged herein apply to and affect Class Members uniformly
2 and Representative Plaintiff’s challenge of these policies and practices hinges on Defendant’s
3 conduct with respect to the Classes in their entirety, not on facts or law applicable only to
4 Representative Plaintiff.

5 28. Unless a Class-wide injunction is issued, Defendant may continue in its failure to
6 properly secure the Private Information of Class Members, and Defendant may continue to act
7 unlawfully as set forth in this Complaint.

8 29. Further, Defendant has acted or refused to act on grounds generally applicable to
9 the Classes and, accordingly, final injunctive or corresponding declaratory relief with regard to the
10 Class Members as a whole is appropriate under Rule 23(b)(2) of the Federal Rules of Civil
11 Procedure.

12 **COMMON FACTUAL ALLEGATIONS**

13 **The Cyberattack**

14 30. In the course of the Data Breach, one or more unauthorized third parties accessed
15 Class Members’ Private Information. Representative Plaintiff was among the individuals whose
16 data was accessed in the Data Breach.

17 31. According to the Data Breach Notification and/or publicly filed documents,
18 Representative Plaintiff states, on information and belief, that thousands/millions of persons were
19 affected by the Data Breach.

20 32. Representative Plaintiff was provided the information detailed above upon
21 Representative Plaintiff’s receipt of a letter from Defendant. Representative Plaintiff was not
22 aware of the Data Breach until receiving that letter.

23 **Defendant’s Failed Response to the Breach**

24 33. Upon information and belief, the unauthorized third-party cybercriminals gained
25 access to Representative Plaintiff’s and Class Members’ Private Information with the intent of
26 misusing the Private Information, including marketing and selling Representative Plaintiff’s and
27 Class Members’ Private Information.
28

COLE & VAN NOTE
ATTORNEYS AT LAW
555 12TH STREET, SUITE 2100
OAKLAND, CA 94607
TEL: (510) 891-9800

1 34. Not until long after it claims to have discovered the Data Breach did Defendant
2 begin sending the Notice to persons whose Private Information Defendant confirmed was
3 potentially compromised as a result of the Data Breach. The Notice provided basic details of the
4 Data Breach and Defendant's recommended next steps.

5 35. Representative Plaintiff and Class Members were required to provide their Private
6 Information to Defendant in order to receive services. Thus, Defendant created, collected and
7 stored Representative Plaintiff's and Class Members' Private Information with the reasonable
8 expectation and mutual understanding that Defendant would comply with its obligations to keep
9 such information confidential and secure from unauthorized access

10 36. Despite this, Representative Plaintiff and the Class Members remain, even today,
11 in the dark regarding what particular data was stolen, the particular malware used and what steps
12 are being taken, if any, to secure their Private Information going forward. Representative Plaintiff
13 and Class Members are thus left to speculate as to where their Private Information ended up, who
14 has used it and for what potentially nefarious purposes. Indeed, they are left to further speculate as
15 to the full impact of the Data Breach and how exactly Defendant intends to enhance its information
16 security systems and monitoring capabilities so as to prevent further breaches.

17 37. Representative Plaintiff's and Class Members' Private Information may end up for
18 sale on the dark web, or simply fall into the hands of companies that will use the detailed Private
19 Information for targeted marketing without Representative Plaintiff's and/or Class Members'
20 approval. Either way, unauthorized individuals can now easily access Representative Plaintiff's
21 and Class Members' Private Information.

22
23 **Defendant Collected/Stored Class Members' Private Information**

24 38. Defendant acquired, collected, stored and assured reasonable security over
25 Representative Plaintiff's and Class Members' Private Information.

26 39. As a condition of its relationships with Representative Plaintiff and Class Members,
27 Defendant required that Representative Plaintiff and Class Members entrust Defendant with highly
28

COLE & VAN NOTE
ATTORNEYS AT LAW
555 12TH STREET, SUITE 2100
OAKLAND, CA 94607
TEL: (510) 891-9800

1 sensitive and confidential Private Information. Defendant, in turn, stored that information on
2 Defendant's system that was ultimately affected by the Data Breach.

3 40. By obtaining, collecting and storing Representative Plaintiff's and Class Members'
4 Private Information, Defendant assumed legal and equitable duties over the Private Information
5 and knew or should have known that it was thereafter responsible for protecting Representative
6 Plaintiff's and Class Members' Private Information from unauthorized disclosure.

7 41. Representative Plaintiff and Class Members have taken reasonable steps to
8 maintain their Private Information's confidentiality. Representative Plaintiff and Class Members
9 relied on Defendant to keep their Private Information confidential and securely maintained, to use
10 this information for business purposes only and to make only authorized disclosures of this
11 information.

12 42. Defendant could have prevented the Data Breach by properly securing and
13 encrypting and/or more securely encrypting its servers generally, as well as Representative
14 Plaintiff's and Class Members' Private Information.

15 43. Defendant's negligence in safeguarding Representative Plaintiff's and Class
16 Members' Private Information is exacerbated by repeated warnings and alerts directed to
17 protecting and securing sensitive data, as evidenced by the trending data breach attacks in recent
18 years.

19 44. Due to the high-profile nature of these breaches, and other breaches of its kind,
20 Defendant was and/or certainly should have been on notice and aware of such attacks occurring in
21 its industry and, therefore, should have assumed and adequately performed the duty of preparing
22 for such an imminent attack. This is especially true given that Defendant is a large, sophisticated
23 operation with the resources to put adequate data security protocols in place.

24 45. And yet, despite the prevalence of public announcements of data breach and data
25 security compromises, Defendant failed to take appropriate steps to protect Representative
26 Plaintiff's and Class Members' Private Information from being compromised.

27
28

COLE & VAN NOTE
 ATTORNEYS AT LAW
 555 12TH STREET, SUITE 2100
 OAKLAND, CA 94607
 TEL: (510) 891-9800

1 **Defendant Had an Obligation to Protect the Stolen Information**

2 46. In failing to adequately secure Representative Plaintiff's and Class Member's
 3 sensitive data, Defendant breached duties it owed Representative Plaintiff and Class Members
 4 under statutory and common law.

5 47. Representative Plaintiff and Class Members surrendered their highly sensitive
 6 Private Information to Defendant under the implied condition that Defendant would keep it private
 7 and secure. Accordingly, Defendant also has an implied duty to safeguard their Private
 8 Information, independent of any statute.

9 48. Defendant was also prohibited by the Federal Trade Commission Act (the "FTC
 10 Act") (15 U.S.C. § 45) from engaging in "unfair or deceptive acts or practices in or affecting
 11 commerce." The Federal Trade Commission (the "FTC") has concluded that a company's failure
 12 to maintain reasonable and appropriate data security for consumers' sensitive personal information
 13 is an "unfair practice" in violation of the FTC Act. *See, e.g., FTC v. Wyndham Worldwide Corp.*,
 14 799 F.3d 236 (3d Cir. 2015).

15 49. In addition to its obligations under federal and state laws, Defendant owed a duty
 16 to Representative Plaintiff and Class Members to exercise reasonable care in obtaining, retaining,
 17 securing, safeguarding, deleting and protecting the Private Information in Defendant's possession
 18 from being compromised, lost, stolen, accessed, and misused by unauthorized persons. Defendant
 19 owed a duty to Representative Plaintiff and Class Members to provide reasonable security,
 20 including consistency with industry standards and requirements, and to ensure that its computer
 21 systems, networks and protocols adequately protected Representative Plaintiff's and Class
 22 Members' Private Information.

23 50. Defendant owed a duty to Representative Plaintiff and Class Members to design,
 24 maintain and test its computer systems, servers and networks to ensure that all Private Information
 25 in its possession was adequately secured and protected.

26 51. Defendant owed a duty to Representative Plaintiff and Class Members to create and
 27 implement reasonable data security practices and procedures to protect all Private Information in
 28

COLE & VAN NOTE
ATTORNEYS AT LAW
555 12TH STREET, SUITE 2100
OAKLAND, CA 94607
TEL: (510) 891-9800

1 its possession, including not sharing information with other entities who maintained sub-standard
2 data security systems.

3 52. Defendant owed a duty to Representative Plaintiff and Class Members to
4 implement processes that would immediately detect a breach of its data security systems in a timely
5 manner.

6 53. Defendant owed a duty to Representative Plaintiff and Class Members to act upon
7 data security warnings and alerts in a timely fashion.

8 54. Defendant owed a duty to Representative Plaintiff and Class Members to disclose
9 if its computer systems and data security practices were inadequate to safeguard individuals’
10 Private Information from theft because such an inadequacy would be a material fact in the decision
11 to entrust their Private Information to Defendant.

12 55. Defendant owed a duty of care to Representative Plaintiff and Class Members
13 because they were foreseeable and probable victims of any inadequate data security practices.

14 56. Defendant owed a duty to Representative Plaintiff and Class Members to encrypt
15 and/or more reliably encrypt Representative Plaintiff’s and Class Members’ Private Information
16 and monitor user behavior and activity in order to identify possible threats.

17

18 **Value of the Relevant Sensitive Information**

19 57. While the greater efficiency of electronic health records translates to cost savings
20 for providers, it also comes with the risk of privacy breaches. These electronic health records
21 contain a plethora of sensitive information (e.g., patient data, patient diagnosis, lab results, medical
22 prescriptions, treatment plans, etc.) that is valuable to cybercriminals. One patient’s complete
23 record can be sold for hundreds of dollars on the dark web. As such, Private Information is a
24 valuable commodity for which a “cyber black market” exists in which criminals openly post stolen
25 payment card numbers, Social Security numbers and other personal information on a number of
26 underground internet websites.

27 58. The high value of Private Information to criminals is further evidenced by the prices
28 they will pay for it through the dark web. Numerous sources cite dark web pricing for stolen

1 identity credentials. For example, personal information can be sold at a price ranging from \$40 to
 2 \$200, and bank details have a price range of \$50 to \$200.³ Experian reports that a stolen credit or
 3 debit card number can sell for \$5 to \$110 on the dark web.⁴ Criminals can also purchase access to
 4 entire company data breaches from \$999 to \$4,995.⁵

5 59. Between 2005 and 2019, at least 249 million people were affected by healthcare
 6 data breaches.⁶ Indeed, during 2019 alone, over 41 million healthcare records were exposed,
 7 stolen, or unlawfully disclosed in 505 data breaches.⁷ In short, these sorts of data breaches are
 8 increasingly common, especially among healthcare systems, which account for 30.03 percent of
 9 overall health data breaches, according to cybersecurity firm Tenable.⁸

10 60. These criminal activities have and will result in devastating financial and personal
 11 losses to Representative Plaintiff and Class Members. For example, it is believed that certain
 12 Private Information compromised in the 2017 Equifax data breach was being used three years later
 13 by identity thieves to apply for COVID-19-related benefits in the state of Oklahoma. Such fraud
 14 will be an omnipresent threat for Representative Plaintiff and Class Members for the rest of their
 15 lives. They will need to remain constantly vigilant.

16 61. The FTC defines identity theft as “a fraud committed or attempted using the
 17 identifying information of another person without authority.” The FTC describes “identifying
 18 information” as “any name or number that may be used, alone or in conjunction with any other
 19 information, to identify a specific person,” including, among other things, “[n]ame, Social Security
 20 number, date of birth, official State or government issued driver’s license or identification number,
 21
 22

23 ³ *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/>

24 ⁴ *Here’s How Much Your Personal Information Is Selling for on the Dark Web*, Experian, Dec.
 6, 2017, available at: <https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/>.

25 ⁵ *In the Dark*, VPNOverview, 2019, available at:
 26 <https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/>.

27 ⁶ <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7349636/#B5-healthcare-08-00133/>.

27 ⁷ <https://www.hipaajournal.com/december-2019-healthcare-data-breach-report/>.

28 ⁸ <https://www.tenable.com/blog/healthcare-security-ransomware-plays-a-prominent-role-in-covid-19-era-breaches/>.

1 alien registration number, government passport number, employer or taxpayer identification
 2 number.”

3 62. Identity thieves can use Private Information, such as that of Representative Plaintiff
 4 and Class Members which Defendant failed to keep secure, to perpetrate a variety of crimes that
 5 harm victims. For instance, identity thieves may commit various types of government fraud such
 6 as immigration fraud, obtaining a driver’s license or identification card in the victim’s name but
 7 with another’s picture, using the victim’s information to obtain government benefits or filing a
 8 fraudulent tax return using the victim’s information to obtain a fraudulent refund.

9 63. The ramifications of Defendant’s failure to keep secure Representative Plaintiff’s
 10 and Class Members’ Private Information are long lasting and severe. Once Private Information is
 11 stolen, particularly identification numbers, fraudulent use of that information and damage to
 12 victims may continue for years. Indeed, Representative Plaintiff’s and Class Members’ Private
 13 Information was taken by hackers to engage in identity theft or to sell it to other criminals who
 14 will purchase the Private Information for that purpose. The fraudulent activity resulting from the
 15 Data Breach may not come to light for years.

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

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

24 65. The harm to Representative Plaintiff and Class Members is especially acute given
 25 the nature of the leaked data. Medical identity theft is one of the most common, most expensive
 26 and most difficult-to-prevent forms of identity theft. According to Kaiser Health News, “medical-
 27 related identity theft accounted for 43 percent of all identity thefts reported in the United States in
 28

⁹ *Report to Congressional Requesters*, GAO, at 29 (June 2007), available at: <http://www.gao.gov/new.items/d07737.pdf>.

1 2013,” which is more than identity thefts involving banking and finance, the government and the
 2 military, or education.¹⁰

3 66. “Medical identity theft is a growing and dangerous crime that leaves its victims
 4 with little to no recourse for recovery,” reported Pam Dixon, executive director of World Privacy
 5 Forum. “Victims often experience financial repercussions and worse yet, they frequently discover
 6 erroneous information has been added to their personal medical files due to the thief’s activities.”¹¹

7 67. When cybercriminals access financial information, health insurance information
 8 and other personally sensitive data—as they did here—there is no limit to the amount of fraud to
 9 which Defendant may have exposed Representative Plaintiff and Class Members.

10 68. A study by Experian found that the average total cost of medical identity theft is
 11 “about \$20,000” per incident, and that a majority of victims of medical identity theft were forced
 12 to pay out-of-pocket costs for healthcare they did not receive in order to restore coverage.¹² Almost
 13 half of medical identity theft victims lose their healthcare coverage as a result of the incident, while
 14 nearly one-third saw their insurance premiums rise, and 40 percent were never able to resolve their
 15 identity theft at all.¹³

16 69. And data breaches are preventable.¹⁴ As Lucy Thompson wrote in the DATA
 17 BREACH AND ENCRYPTION HANDBOOK, “[i]n almost all cases, the data breaches that occurred could
 18 have been prevented by proper planning and the correct design and implementation of appropriate
 19 security solutions.”¹⁵ She added that “[o]rganizations that collect, use, store, and share sensitive
 20 personal data must accept responsibility for protecting the information and ensuring that it is not
 21 compromised....”¹⁶

22
 23 ¹⁰ Michael Ollove, “The Rise of Medical Identity Theft in Healthcare,” Kaiser Health News,
 Feb. 7, 2014, <https://khn.org/news/rise-of-identity-theft/>.

24 ¹¹ *Id.*

25 ¹² Elinor Mills, “Study: Medical Identity Theft is Costly for Victims,” CNET (Mar, 3, 2010),
<https://www.cnet.com/news/study-medical-identity-theft-is-costly-for-victims/>.

26 ¹³ *Id.*; see also Healthcare Data Breach: What to Know About them and What to Do After One,
 EXPERIAN, <https://www.experian.com/blogs/ask-experian/healthcare-data-breach-what-to-know-about-them-and-what-to-do-after-one/>.

27 ¹⁴ Lucy L. Thompson, “Despite the Alarming Trends, Data Breaches Are Preventable,” *in*
 DATA BREACH AND ENCRYPTION HANDBOOK (Lucy Thompson, ed., 2012).

28 ¹⁵ *Id.* at 17.

¹⁶ *Id.* at 28.

COLE & VAN NOTE
ATTORNEYS AT LAW
555 12TH STREET, SUITE 2100
OAKLAND, CA 94607
TEL: (510) 891-9800

1 70. Most of the reported data breaches are a result of lax security and the failure to
2 create or enforce appropriate security policies, rules and procedures. Appropriate information
3 security controls, including encryption, must be implemented and enforced in a rigorous and
4 disciplined manner so that a *data breach never occurs*.¹⁷

5 71. Here, Defendant knew of the importance of safeguarding Private Information and
6 of the foreseeable consequences that would occur if Representative Plaintiff’s and Class Members’
7 Private Information was stolen, including the significant costs that would be placed on
8 Representative Plaintiff and Class Members as a result of a breach of this magnitude. As detailed
9 above, Defendant knew or should have known that the development and use of such protocols
10 were necessary to fulfill its statutory and common law duties to Representative Plaintiff and Class
11 Members. Its failure to do so is therefore intentional, willful, reckless and/or grossly negligent.

12 72. Defendant disregarded the rights of Representative Plaintiff and Class Members by,
13 *inter alia*, (i) intentionally, willfully, recklessly and/or negligently failing to take adequate and
14 reasonable measures to ensure that its network servers were protected against unauthorized
15 intrusions, (ii) failing to disclose that it did not have adequately robust security protocols and
16 training practices in place to adequately safeguard Representative Plaintiff’s and Class Members’
17 Private Information, (iii) failing to take standard and reasonably available steps to prevent the Data
18 Breach, (iv) concealing the existence and extent of the Data Breach for an unreasonable duration
19 of time, and (v) failing to provide Representative Plaintiff and Class Members prompt and accurate
20 notice of the Data Breach.

21
22 **FIRST CLAIM FOR RELIEF**
23 **Negligence**
24 **(On behalf of the Nationwide Class)**

25 73. Each and every allegation of the preceding paragraphs is incorporated in this Count
26 with the same force and effect as though fully set forth herein.

27
28 ¹⁷ *Id.*

COLE & VAN NOTE
ATTORNEYS AT LAW
555 12TH STREET, SUITE 2100
OAKLAND, CA 94607
TEL: (510) 891-9800

1 74. At all times herein relevant, Defendant owed Representative Plaintiff and Class
2 Members a duty of care, *inter alia*, to act with reasonable care to secure and safeguard their Private
3 Information and to use commercially reasonable methods to do so. Defendant took on this
4 obligation upon accepting and storing Representative Plaintiff’s and Class Members’ Private
5 Information on its computer systems.

6 75. Among these duties, Defendant was expected:

- 7 a. to exercise reasonable care in obtaining, retaining, securing, safeguarding,
8 deleting and protecting the Private Information in its possession;
- 9 b. to protect Representative Plaintiff’s and Class Members’ Private
10 Information using reasonable and adequate security procedures and systems
11 that were/are compliant with industry-standard practices;
- 12 c. to implement processes to quickly detect the Data Breach and to timely act
13 on warnings about data breaches; and
- 14 d. to promptly notify Representative Plaintiff and Class Members of any data
15 breach, security incident or intrusion that affected or may have affected their
16 Private Information.

17 76. Defendant knew that the Private Information was private and confidential and
18 should be protected as private and confidential and, thus, Defendant owed a duty of care not to
19 subject Representative Plaintiff and Class Members to an unreasonable risk of harm because they
20 were foreseeable and probable victims of any inadequate security practices.

21 77. Defendant knew or should have known of the risks inherent in collecting and
22 storing Private Information, the vulnerabilities of its data security systems and the importance of
23 adequate security. Defendant knew about numerous, well-publicized data breaches.

24 78. Defendant knew or should have known that its data systems and networks did not
25 adequately safeguard Representative Plaintiff’s and Class Members’ Private Information.

26 79. Only Defendant was in the position to ensure that its systems and protocols were
27 sufficient to protect the Private Information that Representative Plaintiff and Class Members had
28 entrusted to it.

 80. Defendant breached its duties to Representative Plaintiff and Class Members by
failing to provide fair, reasonable or adequate computer systems and data security practices to
safeguard Representative Plaintiff’s and Class Members’ Private Information.

1 81. Because Defendant knew that a breach of its systems could damage thousands of
 2 individuals, including Representative Plaintiff and Class Members, Defendant had a duty to
 3 adequately protect its data systems and the Private Information contained thereon.

4 82. Representative Plaintiff's and Class Members' willingness to entrust Defendant
 5 with its Private Information was predicated on the understanding that Defendant would take
 6 adequate security precautions. Moreover, only Defendant had the ability to protect its systems and
 7 the Private Information it stored on them from attack. Thus, Defendant had a special relationship
 8 with Representative Plaintiff and Class Members.

9 83. Defendant also had independent duties under state and federal laws that required
 10 Defendant to reasonably safeguard Representative Plaintiff's and Class Members' Private
 11 Information and promptly notify them about the Data Breach. These "independent duties" are
 12 untethered to any contract between Defendant and Representative Plaintiff and/or the remaining
 13 Class Members.

14 84. Defendant breached its general duty of care to Representative Plaintiff and Class
 15 Members in, but not necessarily limited to, the following ways:

- 16 a. by failing to provide fair, reasonable or adequate computer systems and data
 17 security practices to safeguard Representative Plaintiff's and Class
 Members' Private Information;
- 18 b. by failing to timely and accurately disclose that Representative Plaintiff's
 19 and Class Members' Private Information had been improperly acquired or
 accessed;
- 20 c. by failing to adequately protect and safeguard the Private Information by
 21 knowingly disregarding standard information security principles, despite
 obvious risks, and by allowing unmonitored and unrestricted access to
 22 unsecured Private Information;
- 23 d. by failing to provide adequate supervision and oversight of the Private
 24 Information with which it was and is entrusted, in spite of the known risk
 and foreseeable likelihood of breach and misuse, which permitted an
 25 unknown third party to gather Representative Plaintiff's and Class
 Members' Private Information, misuse the Private Information and
 intentionally disclose it to others without consent;
- 26 e. by failing to adequately train its employees to not store Private Information
 27 longer than absolutely necessary;
- 28 f. by failing to consistently enforce security policies aimed at protecting
 Representative Plaintiff's and the Class Members' Private Information;

COLE & VAN NOTE
ATTORNEYS AT LAW
555 12TH STREET, SUITE 2100
OAKLAND, CA 94607
TEL: (510) 891-9800

- 1 g. by failing to implement processes to quickly detect data breaches, security
- 2 incidents or intrusions; and
- 3 h. by failing to encrypt Representative Plaintiff's and Class Members' Private
- 4 Information and monitor user behavior and activity in order to identify
- 5 possible threats.

6 85. Defendant's willful failure to abide by these duties was wrongful, reckless and/or

7 grossly negligent in light of the foreseeable risks and known threats.

8 86. As a proximate and foreseeable result of Defendant's grossly negligent conduct,

9 Representative Plaintiff and Class Members have suffered damages and are at imminent risk of

10 additional harms and damages (as alleged above).

11 87. The law further imposes an affirmative duty on Defendant to timely disclose the

12 unauthorized access and theft of the Private Information to Representative Plaintiff and Class

13 Members so that they could and/or still can take appropriate measures to mitigate damages, protect

14 against adverse consequences and thwart future misuse of their Private Information.

15 88. Defendant breached its duty to notify Representative Plaintiff and Class Members

16 of the unauthorized access by waiting excessively after learning of the Data Breach to notify

17 Representative Plaintiff and Class Members and then by failing and continuing to fail to provide

18 Representative Plaintiff and Class Members sufficient information regarding the breach. To date,

19 Defendant has not provided sufficient information to Representative Plaintiff and Class Members

20 regarding the extent of the unauthorized access and continues to breach its disclosure obligations

21 to Representative Plaintiff and Class Members.

22 89. Further, through its failure to provide timely and clear notification of the Data

23 Breach to Representative Plaintiff and Class Members, Defendant prevented Representative

24 Plaintiff and Class Members from taking meaningful, proactive steps to, *inter alia*, secure and/or

25 access their Private Information.

26 90. There is a close causal connection between Defendant's failure to implement

27 security measures to protect Representative Plaintiff's and Class Members' Private Information

28 and the harm suffered, or risk of imminent harm suffered, by Representative Plaintiff and Class

Members. Representative Plaintiff's and Class Members' Private Information was accessed as the

COLE & VAN NOTE
ATTORNEYS AT LAW
555 12TH STREET, SUITE 2100
OAKLAND, CA 94607
TEL: (510) 891-9800

1 proximate result of Defendant’s failure to exercise reasonable care in safeguarding such Private
2 Information by adopting, implementing and maintaining appropriate security measures.

3 91. Defendant’s wrongful actions, inactions and omissions constituted (and continue to
4 constitute) common law negligence.

5 92. The damages Representative Plaintiff and Class Members have suffered (as alleged
6 above) and will continue to suffer were and are the direct and proximate result of Defendant’s
7 grossly negligent conduct.

8 93. Additionally, 15 U.S.C. § 45 (FTC Act, Section 5) prohibits “unfair [...] practices
9 in or affecting commerce,” including, as interpreted and enforced by the FTC, the unfair act or
10 practice by businesses, such as Defendant, of failing to use reasonable measures to protect Private
11 Information. The FTC publications and orders described above also form part of the basis of
12 Defendant’s duty in this regard.

13 94. Defendant violated 15 U.S.C. § 45 by failing to use reasonable measures to protect
14 Private Information and not complying with applicable industry standards, as described in detail
15 herein. Defendant’s conduct was particularly unreasonable given the nature and amount of Private
16 Information it obtained and stored and the foreseeable consequences of the immense damages that
17 would result to Representative Plaintiff and Class Members.

18 95. As a direct and proximate result of Defendant’s negligence, Representative Plaintiff
19 and Class Members have suffered and will continue to suffer injury, including, but not limited to,
20 (i) actual identity theft, (ii) the loss of the opportunity of how their Private Information is used,
21 (iii) the compromise, publication and/or theft of their Private Information, (iv) out-of-pocket
22 expenses associated with the prevention, detection and recovery from identity theft, tax fraud
23 and/or unauthorized use of their Private Information, (v) lost opportunity costs associated with
24 effort expended and the loss of productivity addressing and attempting to mitigate the actual and
25 future consequences of the Data Breach, including, but not limited to, efforts spent researching
26 how to prevent, detect, contest and recover from embarrassment and identity theft, (vi) lost
27 continuity in relation to their personal records, (vii) the continued risk to their Private Information,
28 which may remain in Defendant’s possession and is subject to further unauthorized disclosures so

COLE & VAN NOTE
ATTORNEYS AT LAW
555 12TH STREET, SUITE 2100
OAKLAND, CA 94607
TEL: (510) 891-9800

1 long as Defendant fails to undertake appropriate and adequate measures to protect Representative
2 Plaintiff's and Class Members' Private Information in its continued possession, and (viii) future
3 costs in terms of time, effort and money that will be expended to prevent, detect, contest and repair
4 the impact of the Private Information compromised as a result of the Data Breach for the remainder
5 of the lives of Representative Plaintiff and Class Members.

6 96. As a direct and proximate result of Defendant's negligence, Representative Plaintiff
7 and Class Members have suffered and will continue to suffer other forms of injury and/or harm,
8 including, but not limited to, anxiety, emotional distress, loss of privacy and other economic and
9 noneconomic losses.

10 97. Additionally, as a direct and proximate result of Defendant's negligence,
11 Representative Plaintiff and Class Members have suffered and will continue to suffer the continued
12 risks of exposure of their Private Information, which remains in Defendant's possession and is
13 subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and
14 adequate measures to protect Private Information in its continued possession.

15
16 **SECOND CLAIM FOR RELIEF**
17 **Breach of Implied Contract**
18 **(On behalf of the Nationwide Class)**

19 98. Each and every allegation of the preceding paragraphs is incorporated in this Count
20 with the same force and effect as though fully set forth herein.

21 99. Through their course of conduct, Defendant, Representative Plaintiff and Class
22 Members entered into implied contracts for Defendant to implement data security adequate to
23 safeguard and protect the privacy of Representative Plaintiff's and Class Members' Private
24 Information.

25 100. Defendant solicited, invited and required Representative Plaintiff and Class
26 Members to provide their Private Information as part of Defendant's regular business practices.
27 Representative Plaintiff and Class Members accepted Defendant's offers by, in part, providing
28 their Private Information to Defendant.

COLE & VAN NOTE
ATTORNEYS AT LAW
555 12TH STREET, SUITE 2100
OAKLAND, CA 94607
TEL: (510) 891-9800

1 101. As a condition of being direct customers and/or employees of Defendant,
2 Representative Plaintiff and Class Members provided and entrusted their Private Information to
3 Defendant. In so doing, Representative Plaintiff and Class Members entered into implied contracts
4 with Defendant by which Defendant agreed to safeguard and protect such non-public information,
5 to keep such information secure and confidential and to timely and accurately notify
6 Representative Plaintiff and Class Members if its data had been breached and compromised or
7 stolen.

8 102. A meeting of the minds occurred when Representative Plaintiff and Class Members
9 agreed to, and did, provide their Private Information to Defendant, in exchange for, amongst other
10 things, the protection of their Private Information.

11 103. Representative Plaintiff and Class Members fully performed their obligations under
12 the implied contracts with Defendant.

13 104. Defendant breached the implied contracts it made with Representative Plaintiff and
14 Class Members by failing to safeguard and protect their Private Information and by failing to
15 provide timely and accurate notice to them that their Private Information was compromised as a
16 result of the Data Breach.

17 105. As a direct and proximate result of Defendant's above-described breach of implied
18 contract, Representative Plaintiff and Class Members have suffered and will continue to suffer (i)
19 ongoing, imminent and impending threat of identity theft crimes, fraud and abuse, resulting in
20 monetary loss and economic harm, (ii) actual identity theft crimes, fraud and abuse, resulting in
21 monetary loss and economic harm, (iii) loss of the confidentiality of the stolen confidential data,
22 (iv) the illegal sale of the compromised data on the dark web, (v) lost work time, and (f) other
23 economic and noneconomic harm.

24 **THIRD CLAIM FOR RELIEF**
25 **Breach of the Implied Covenant of Good Faith and Fair Dealing**
26 **(On behalf of the Nationwide Class)**

27 106. Each and every allegation of the preceding paragraphs is incorporated in this Count
28 with the same force and effect as though fully set forth therein.

COLE & VAN NOTE
ATTORNEYS AT LAW
555 12TH STREET, SUITE 2100
OAKLAND, CA 94607
TEL: (510) 891-9800

1 107. Every contract in this State has an implied covenant of good faith and fair
2 dealing. This implied covenant is an independent duty and may be breached even when there
3 is no breach of a contract's actual and/or express terms.

4 108. Representative Plaintiff and Class Members have complied with and performed all
5 conditions of their contracts with Defendant.

6 109. Defendant breached the implied covenant of good faith and fair dealing by failing
7 to maintain adequate computer systems and data security practices to safeguard Private
8 Information, failing to timely and accurately disclose the Data Breach to Representative Plaintiff
9 and Class Members and continued acceptance of Private Information and storage of other personal
10 information after Defendant knew or should have known of the security vulnerabilities of the
11 systems that were exploited in the Data Breach.

12 110. Defendant acted in bad faith and/or with malicious motive in denying
13 Representative Plaintiff and Class Members the full benefit of their bargains as originally intended
14 by the parties, thereby causing them injury in an amount to be determined at trial.

15
16 **RELIEF SOUGHT**

17 **WHEREFORE**, Representative Plaintiff, on Representative Plaintiff's own behalf and on
18 behalf of each member of the proposed National Class, respectfully requests that the Court enter
19 judgment in favor of Representative Plaintiff and the Class and for the following specific relief
20 against Defendant as follows:

21 1. That the Court declare, adjudge and decree that this action is a proper class action
22 and certify the proposed Class and/or any other appropriate subclasses under Federal Rules of Civil
23 Procedure Rule 23 (b)(1), (b)(2), and/or (b)(3), including appointment of Representative Plaintiff's
24 counsel as Class Counsel;

25 2. For an award of damages, including actual, nominal and consequential damages, as
26 allowed by law in an amount to be determined;

27 3. That the Court enjoin Defendant, ordering it to cease and desist from unlawful
28 activities;

COLE & VAN NOTE
ATTORNEYS AT LAW
555 12TH STREET, SUITE 2100
OAKLAND, CA 94607
TEL: (510) 891-9800

1 4. For equitable relief enjoining Defendant from engaging in the wrongful conduct
2 complained of herein pertaining to the misuse and/or disclosure of Representative Plaintiff's and
3 Class Members' Private Information, and from refusing to issue prompt, complete and accurate
4 disclosures to Representative Plaintiff and Class Members;

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

- 8 a. prohibiting Defendant from engaging in the wrongful and unlawful acts
9 described herein;
- 10 b. requiring Defendant to protect, including through encryption, all data
11 collected through the course of business in accordance with all applicable
12 regulations, industry standards and federal, state or local laws;
- 13 c. requiring Defendant to delete and purge Representative Plaintiff's and Class
14 Members' Private Information unless Defendant can provide to the Court
15 reasonable justification for the retention and use of such information when
16 weighed against the privacy interests of Representative Plaintiff and Class
17 Members;
- 18 d. requiring Defendant to implement and maintain a comprehensive
19 Information Security Program designed to protect the confidentiality and
20 integrity of Representative Plaintiff's and Class Members' Private
21 Information;
- 22 e. requiring Defendant to engage independent third-party security auditors and
23 internal personnel to run automated security monitoring, simulated attacks,
24 penetration tests and audits on Defendant's systems on a periodic basis;
- 25 f. prohibiting Defendant from maintaining Representative Plaintiff's and
26 Class Members' Private Information on a cloud-based database;
- 27 g. requiring Defendant to segment data by creating firewalls and access
28 controls so that if one area of Defendant's network is compromised, hackers
cannot gain access to other portions of Defendant's systems;
- h. requiring Defendant to conduct regular database scanning and securing
checks;
- i. requiring Defendant to establish an information security training program
that includes at least annual information security training for all employees,
with additional training to be provided as appropriate based upon the
employees' respective responsibilities with handling Private Information,
as well as protecting the Private Information of Representative Plaintiff and
Class Members;
- j. requiring Defendant to implement a system of tests to assess its respective
employees' knowledge of the education programs discussed in the

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

preceding subparagraphs, as well as randomly and periodically testing employees' compliance with Defendant's policies, programs and systems for protecting personal identifying information;

k. requiring Defendant to implement, maintain, review and revise as necessary a threat management program to appropriately monitor Defendant's networks for internal and external threats, and assess whether monitoring tools are properly configured, tested and updated; and

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

6. For prejudgment interest on all amounts awarded, at the prevailing legal rate;

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

and

8. For all other Orders, findings and determinations identified and sought in this

Complaint.

JURY DEMAND

Representative Plaintiff, individually and on behalf of the Plaintiff Class and/or subclasses, hereby demands a trial by jury for all issues triable by jury.

Dated: July 1, 2024

By: /s/ Scott Edward Cole
Scott Edward Cole, Esq. (S.B. #160744)
Laura Grace Van Note, Esq. (S.B. #310160)
COLE & VAN NOTE
555 12th Street, Suite 2100
Oakland, California 94607
Telephone: (510) 891-9800
Facsimile: (510) 891-7030
Email: sec@colevannote.com
Email: lvn@colevannote.com

Attorneys for Representative Plaintiff and the Plaintiff Class

COLE & VAN NOTE
ATTORNEYS AT LAW
555 12TH STREET, SUITE 2100
OAKLAND, CA 94607
TEL: (510) 891-9800