

1 Scott Edward Cole, Esq. (S.B. #160744)
Laura Grace Van Note, Esq. (S.B. #310160)
2 Cody Alexander Bolce, Esq. (S.B. #322725)
COLE & VAN NOTE
3 555 12th Street, Suite 1725
Oakland, California 94607
4 Telephone: (510) 891-9800
Facsimile: (510) 891-7030
5 Email: sec@colevannote.com
Email: lvn@colevannote.com
6 Email: cab@colevannote.com
Web: www.colevannote.com
7

8 Attorneys for Representative Plaintiff
and the Plaintiff Class
9

10 **UNITED STATES DISTRICT COURT**
11 **NORTHERN DISTRICT OF CALIFORNIA**
12

13 SABRINA SINGLETON, individually, and
on behalf of all others similarly situated,
14

Plaintiff,
15

vs.
16

BLACKHAWK NETWORK, INC. dba
BLACKHAWK ENGAGEMENT
SOLUTIONS,
17

Defendant.
18
19
20
21

Case No.

CLASS ACTION

**COMPLAINT FOR DAMAGES,
INJUNCTIVE AND EQUITABLE RELIEF
FOR:**

- 1. NEGLIGENCE;
- 2. BREACH OF CONFIDENCE;
- 3. BREACH OF IMPLIED CONTRACT;
- 4. BREACH OF IMPLIED COVENANT OF
GOOD FAITH AND FAIR DEALING;

[JURY TRIAL DEMANDED]
22
23
24
25
26
27
28

COLE & VAN NOTE
ATTORNEYS AT LAW
555 12TH STREET, SUITE 1725
OAKLAND, CA 94607
TEL: (510) 891-9800

1 Representative Plaintiff alleges as follows:
2

3 **INTRODUCTION**

4 1. Representative Plaintiff SABRINA SINGLETON (“Representative Plaintiff”),
5 brings this class action against Defendant BLACKHAWK NETWORK, INC. dba
6 BLACKHAWK ENGAGEMENT SOLUTIONS (“Defendant” or “BLACKHAWK”) for its
7 failure to properly secure and safeguard Representative Plaintiff’s and Class Members’ personally
8 identifiable information stored within Defendant’s information network, including, without
9 limitation, first and last names, email addresses, phone numbers, payment card data in combination
10 with information related to the Prepaid Card profiles, which includes, but is not limited to,
11 information added by customers to PrepaidCenter.com, such as card numbers, expiration dates,
12 and CVV security codes (these types of information, *inter alia*, being thereafter referred to,
13 collectively, as “personally identifiable information” or “PII”).¹

14 2. With this action, Representative Plaintiff seeks to hold Defendant responsible for
15 the harms it caused and will continue to cause Representative Plaintiff and, at least, 165,000² others
16 similarly situated persons in the massive and preventable cyberattack purportedly discovered by
17 Defendant on September 11, 2022, by which cybercriminals infiltrated Defendant’s inadequately
18 protected network servers and accessed highly sensitive PII and financial information which was
19 being kept unprotected (the “Data Breach”).

20 3. Representative Plaintiff further seeks to hold Defendant responsible for not
21 ensuring that the PII was maintained in a manner consistent with industry and other relevant
22 standards.
23

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

² <https://apps.web.maine.gov/online/aeviewer/ME/40/52a7dc3e-1734-4ea7-b1a8-6e8d49176588.shtml> (last accessed November 15, 2022).

COLE & VAN NOTE
ATTORNEYS AT LAW
555 12TH STREET, SUITE 1725
OAKLAND, CA 94607
TEL: (510) 891-9800

COLE & VAN NOTE
ATTORNEYS AT LAW
555 12TH STREET, SUITE 1725
OAKLAND, CA 94607
TEL: (510) 891-9800

1 U.S.C. § 1332(d) because this is a class action where the amount in controversy exceeds the sum
2 or value of \$5 million, exclusive of interest and costs, there are more than 100 members in the
3 proposed class, and at least one other Class Member is a citizen of a state different from Defendant.

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

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

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

13
14 **PLAINTIFF**

15 12. Representative Plaintiff is an adult individual and, at all relevant times herein, a
16 resident of the state of New York. Representative Plaintiff is a victim of the Data Breach.

17 13. Defendant received highly sensitive personal and financial information from
18 Representative Plaintiff in connection with the gift cards, prepaid incentive cards, and other online
19 payment options it provides. As a result, Representative Plaintiff’s information was among the
20 data accessed by an unauthorized third-party in the Data Breach.

21 14. Representative Plaintiff received—and was a “consumer” for purposes of obtaining
22 services from Defendant.

23 15. At all times herein relevant, Representative Plaintiff is and was a member of each
24 of the Classes.

25 16. As required in order to obtain services from Defendant, Representative Plaintiff
26 provided Defendant with highly sensitive personal and financial information.

27
28

COLE & VAN NOTE
ATTORNEYS AT LAW
555 12TH STREET, SUITE 1725
OAKLAND, CA 94607
TEL: (510) 891-9800

1 17. Representative Plaintiff’s PII was exposed in the Data Breach because Defendant
2 stored and/or shared Representative Plaintiff’s PII and financial information. Her PII and financial
3 information was within the possession and control of Defendant at the time of the Data Breach.

4 18. Representative Plaintiff received a letter from Defendant, dated on or about October
5 31, 2022, stating that her PII and financial information was involved in the Data Breach (the
6 “Notice”).

7 19. 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 her accounts and seeking legal counsel regarding her options for remedying and/or
11 mitigating the effects of the Data Breach. This time has been lost forever and cannot be recaptured.

12 20. Representative Plaintiff suffered actual injury in the form of damages to and
13 diminution in the value of her PII—a form of intangible property that she entrusted to Defendant,
14 which was compromised in and as a result of the Data Breach.

15 21. Representative Plaintiff suffered lost time, annoyance, interference, and
16 inconvenience as a result of the Data Breach and has anxiety and increased concerns for the loss
17 of privacy, as well as anxiety over the impact of cybercriminals accessing, using, and selling her
18 PII and/or financial information.

19 22. Representative Plaintiff has suffered imminent and impending injury arising from
20 the substantially increased risk of fraud, identity theft, and misuse resulting from her PII and
21 financial information, in combination with her name, being placed in the hands of unauthorized
22 third parties/criminals.

23 23. Representative Plaintiff has a continuing interest in ensuring that her PII, which,
24 upon information and belief, remains backed up in Defendant’s possession, is protected and
25 safeguarded from future breaches.

26
27
28

DEFENDANT

24. Defendant Blackhawk Network, Inc. dba Blackhawk Engagement Solutions is a California corporation with a principal place of business located at 6220 Stoneridge Mall Rd, Pleasanton, CA 94588.

25. Defendant provides gift cards, prepaid incentive cards, and other online payment options for employers and merchants located within the United States and abroad.³

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

CLASS ACTION ALLEGATIONS

27. Representative Plaintiff brings this action pursuant to the provisions of Rules 23(a), (b)(2), and (b)(3) of the Federal Rules of Civil Procedure, on behalf of herself and the following classes:

Nationwide Class:

“All individuals within the United States of America whose PII and/or financial information was exposed to unauthorized third-parties as a result of the data breach discovered by Defendant on September 11, 2022.”

California Subclass:

“All individuals within the State of California whose PII and/or financial information was exposed to unauthorized third-parties as a result of the data breach discovered by Defendant on September 11, 2022”

28. Excluded from the Classes are the following individuals and/or entities: Defendant and Defendant’s parents, subsidiaries, affiliates, officers and directors, and any entity in which Defendant has a controlling interest; all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out; any and all federal, state or local governments, including but not limited to its departments, agencies, divisions, bureaus, boards,

³ <https://blackhawknetwork.com> (last accessed November 15, 2022)

COLE & VAN NOTE
ATTORNEYS AT LAW
555 12TH STREET, SUITE 1725
OAKLAND, CA 94607
TEL: (510) 891-9800

COLE & VAN NOTE
ATTORNEYS AT LAW
555 12TH STREET, SUITE 1725
OAKLAND, CA 94607
TEL: (510) 891-9800

1 sections, groups, counsels and/or subdivisions; and all judges assigned to hear any aspect of this
2 litigation, as well as its immediate family members.

3 29. Also, in the alternative, Representative Plaintiff requests additional Subclasses as
4 necessary based on the types of PII that were compromised.

5 30. Representative Plaintiff reserves the right to amend the above definition or to
6 propose subclasses in subsequent pleadings and motions for class certification.

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

10 a. Numerosity: A class action is the only available method for the fair and
11 efficient adjudication of this controversy. The members of the Plaintiff
12 Classes are so numerous that joinder of all members is impractical, if not
13 impossible. Representative Plaintiff is informed and believes and, on that
14 basis, alleges that the total number of Class Members is in the hundreds of
15 thousands of individuals. Membership in the classes will be determined by
16 analysis of Defendant’s records.

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

- 22 1) Whether Defendant had a legal duty to Representative Plaintiff and the
23 Classes to exercise due care in collecting, storing, using and/or
24 safeguarding their PII;
- 25 2) Whether Defendant knew or should have known of the susceptibility
26 of its data security systems to a data breach;
- 27 3) Whether Defendant’s security procedures and practices to protect its
28 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 PII had been
compromised;
- 7) How and when Defendant actually learned of the Data Breach;

COLE & VAN NOTE
ATTORNEYS AT LAW
555 12TH STREET, SUITE 1725
OAKLAND, CA 94607
TEL: (510) 891-9600

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

- 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 the PII of Representative Plaintiff and Class Members;
- 9) Whether Defendant adequately addressed and fixed the vulnerabilities which permitted the Data Breach to occur;
- 10) Whether Defendant engaged in unfair, unlawful, or deceptive practices by failing to safeguard the PII of Representative Plaintiff and Class Members;
- 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;
- 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 are adequate representatives 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, are committed to vigorous prosecution of this case and have 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 its 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.

32. 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

COLE & VAN NOTE
ATTORNEYS AT LAW
555 12TH STREET, SUITE 1725
OAKLAND, CA 94607
TEL: (510) 891-9800

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

6 33. Unless a Class-wide injunction is issued, Defendant may continue in its failure to
7 properly secure the PII and/or financial information of Class Members, and Defendant may
8 continue to act unlawfully as set forth in this Complaint.

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

13 **COMMON FACTUAL ALLEGATIONS**

14 **The Cyberattack**

15 35. In the course of the Data Breach, one or more unauthorized third-parties accessed
16 Class Members’ sensitive data including, but not limited to, first and last names, email addresses,
17 phone numbers, payment card data in combination with information related to the Prepaid Card
18 profiles, which includes, but is not limited to, information added by customers to
19 PrepaidCenter.com, such as card numbers, expiration dates, and CVV security codes.
20 Representative Plaintiff was among the individuals whose data was accessed in the Data Breach.

21 36. Representative Plaintiff was provided the information detailed above upon their
22 receipt of a letter from Defendant, dated on or about October 31, 2022. Representative Plaintiff
23 was not aware of the Data Breach—or even that Defendant was still in possession of her data until
24 receiving that letter.

25
26 **Defendant’s Failed Response to the Breach**

27 37. Upon information and belief, the unauthorized third-party cybercriminals gained
28 access to Representative Plaintiff’s and Class Members’ PII and financial information with the

COLE & VAN NOTE
ATTORNEYS AT LAW
555 12TH STREET, SUITE 1725
OAKLAND, CA 94607
TEL: (510) 891-9800

1 | intent of engaging in misuse of the PII and financial information, including marketing and selling
2 | Representative Plaintiff's and Class Members' PII.

3 | 38. Not until roughly two months after it claims to have discovered the Data Breach
4 | did Defendant begin sending the Notice to persons whose PII and/or financial information
5 | Defendant confirmed was potentially compromised as a result of the Data Breach. The Notice
6 | provided basic details of the Data Breach and Defendant's recommended next steps.

7 | 39. The Notice included, *inter alia*, the claims that Defendant had learned of the Data
8 | Breach on September 11, 2022 and had taken steps to respond. However, it did not state when or
9 | for how long the Data Breach occurred.

10 | 40. Upon information and belief, the unauthorized third-party cybercriminals gained
11 | access to Representative Plaintiff's and Class Members' PII and financial information with the
12 | intent of engaging in misuse of the PII and financial information, including marketing and selling
13 | Representative Plaintiff's and Class Members' PII.

14 | 41. Defendant had and continues to have obligations created by applicable federal and
15 | state laws as set forth herein, reasonable industry standards, common law, and its own assurances
16 | and representations to keep Representative Plaintiff's and Class Members' PII confidential and to
17 | protect such PII from unauthorized access.

18 | 42. Representative Plaintiff and Class Members were required to provide their PII and
19 | financial information to Defendant in order to receive payment services, and as part of providing
20 | such services, Defendant created, collected, and stored Representative Plaintiff and Class
21 | Members PII and financial information with the reasonable expectation and mutual understanding
22 | that Defendant would comply with its obligations to keep such information confidential and secure
23 | from unauthorized access.

24 | 43. Despite this, Representative Plaintiff and the Class Members remain, even today,
25 | in the dark regarding what particular data was stolen, the particular malware used, and what steps
26 | are being taken, if any, to secure their PII and financial information going forward. Representative
27 | Plaintiff and Class Members are, thus, left to speculate as to where their PII ended up, who has
28 | used it, and for what potentially nefarious purposes. Indeed, they are left to further speculate as to

COLE & VAN NOTE
ATTORNEYS AT LAW
555 12TH STREET, SUITE 1725
OAKLAND, CA 94607
TEL: (510) 891-9800

1 the full impact of the Data Breach and how exactly Defendant intend to enhance its information
2 security systems and monitoring capabilities so as to prevent further breaches.

3 44. Representative Plaintiff's and Class Members' PII and financial information may
4 end up for sale on the dark web, or simply fall into the hands of companies that will use the detailed
5 PII and financial information for targeted marketing without the approval of Representative
6 Plaintiff and/or Class Members. Either way, unauthorized individuals can now easily access the
7 PII and financial information of Representative Plaintiff and Class Members.

8
9 **Defendant Collected/Stored Class Members' PII and Financial Information**

10 45. Defendant acquired, collected, and stored and assured reasonable security over
11 Representative Plaintiff's and Class Members' PII and financial information.

12 46. As a condition of its relationships with Representative Plaintiff and Class Members,
13 Defendant required that Representative Plaintiff and Class Members entrust Defendant with highly
14 sensitive and confidential PII and financial information. Defendant, in turn, stored that information
15 of Defendant's system that was ultimately affected by the Data Breach.

16 47. By obtaining, collecting, and storing Representative Plaintiff's and Class Members'
17 PII and financial information, Defendant assumed legal and equitable duties and knew or should
18 have known that they were thereafter responsible for protecting Representative Plaintiff's and
19 Class Members' PII and financial information from unauthorized disclosure.

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

25 49. Defendant could have prevented the Data Breach, which began as early as
26 September 11, 2022, by properly securing and encrypting and/or more securely encrypting its
27 servers generally, as well as Representative Plaintiff's and Class Members' PII and financial
28 information.

1 50. Defendant’s negligence in safeguarding Representative Plaintiff’s and Class
 2 Members’ PII and financial information is exacerbated by repeated warnings and alerts directed to
 3 protecting and securing sensitive data, as evidenced by the trending data breach attacks in recent
 4 years.

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

10 52. Yet, despite the prevalence of public announcements of data breach and data
 11 security compromises, Defendant failed to take appropriate steps to protect Representative
 12 Plaintiff’s and Class Members’ PII and financial information from being compromised.

13
 14 **Defendant Had an Obligation to Protect the Stolen Information**

15 53. Defendant’s failure to adequately secure Representative Plaintiff’s and Class
 16 Members’ sensitive data breaches duties it owes Representative Plaintiff and Class Members under
 17 statutory and common law. Defendant has a statutory duty under federal and state statutes to
 18 safeguard Representative Plaintiff’s and Class Members’ data. Moreover, Representative Plaintiff
 19 and Class Members surrendered their highly sensitive personal data to Defendant under the implied
 20 condition that Defendant would keep it private and secure. Accordingly, Defendant also has an
 21 implied duty to safeguard their data, independent of any statute

22 54. Defendant was also prohibited by the Federal Trade Commission Act (the “FTC
 23 Act”) (15 U.S.C. § 45) from engaging in “unfair or deceptive acts or practices in or affecting
 24 commerce.” The Federal Trade Commission (the “FTC”) has concluded that a company’s failure
 25 to maintain reasonable and appropriate data security for consumers’ sensitive personal information
 26 is an “unfair practice” in violation of the FTC Act. See, e.g., *FTC v. Wyndham Worldwide Corp.*,
 27 799 F.3d 236 (3d Cir. 2015).

COLE & VAN NOTE
ATTORNEYS AT LAW
555 12TH STREET, SUITE 1725
OAKLAND, CA 94607
TEL: (510) 891-9800

1 55. In addition to its obligations under federal and state laws, Defendant owed a duty
2 to Representative Plaintiff and Class Members to exercise reasonable care in obtaining, retaining,
3 securing, safeguarding, deleting, and protecting the PII and financial information in Defendant's
4 possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons.
5 Defendant owed a duty to Representative Plaintiff and Class Members to provide reasonable
6 security, including consistency with industry standards and requirements, and to ensure that its
7 computer systems, networks, and protocols adequately protected the PII and financial information
8 of Representative Plaintiff and Class Members.

9 56. Defendant owed a duty to Representative Plaintiff and Class Members to design,
10 maintain, and test its computer systems, servers, and networks to ensure that the PII and financial
11 information in its possession was adequately secured and protected.

12 57. Defendant owed a duty to Representative Plaintiff and Class Members to create and
13 implement reasonable data security practices and procedures to protect the PII and financial
14 information in its possession, including not sharing information with other/her/their entities who
15 maintained sub-standard data security systems.

16 58. Defendant owed a duty to Representative Plaintiff and Class Members to
17 implement processes that would immediately detect a breach on its data security systems in a
18 timely manner.

19 59. Defendant owed a duty to Representative Plaintiff and Class Members to act upon
20 data security warnings and alerts in a timely fashion.

21 60. Defendant owed a duty to Representative Plaintiff and Class Members to disclose
22 if its computer systems and data security practices were inadequate to safeguard individuals' PII
23 and/or financial information from theft because such an inadequacy would be a material fact in the
24 decision to entrust this PII and/or financial information to Defendant.

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

27
28

1 62. Defendant owed a duty to Representative Plaintiff and Class Members to encrypt
2 and/or more reliably encrypt Representative Plaintiff's and Class Members' PII and financial
3 information and monitor user behavior and activity in order to identify possible threats.

4
5 **Value of the Relevant Sensitive Information**

6 63. PII and financial information are valuable commodities for which a "cyber black
7 market" exists in which criminals openly post stolen payment card numbers, Social Security
8 numbers, and other personal information on a number of underground internet websites.

9 64. The high value of PII and financial information to criminals is further evidenced by
10 the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen
11 identity credentials. For example, personal information can be sold at a price ranging from \$40 to
12 \$200, and bank details have a price range of \$50 to \$200.⁴ Experian reports that a stolen credit or
13 debit card number can sell for \$5 to \$110 on the dark web.⁵ Criminals can also purchase access to
14 entire company data breaches from \$999 to \$4,995.⁶

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

21 66. The FTC defines identity theft as "a fraud committed or attempted using the
22 identifying information of another person without authority." The FTC describes "identifying
23 information" as "any name or number that may be used, alone or in conjunction with any other

24 ⁴ *Your personal data is for sale on the dark web. Here's how much it costs*, Digital Trends, Oct.
25 16, 2019, available at: <https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/> (last accessed July 28, 2021).

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

28 ⁶ *In the Dark*, VPNOverview, 2019, available at: <https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/> (last accessed January 21, 2022).

1 information, to identify a specific person,” including, among other things, “[n]ame, Social Security
 2 number, date of birth, official State or government issued driver’s license or identification number,
 3 alien registration number, government passport number, employer or taxpayer identification
 4 number.”

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

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

19 69. There may be a time lag between when harm occurs versus when it is discovered,
 20 and also between when PII and/or financial information is stolen and when it is used. According
 21 to the U.S. Government Accountability Office (“GAO”), which conducted a study regarding data
 22 breaches:

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

28 ⁷ *Report to Congressional Requesters*, GAO, at 29 (June 2007), available at:
<http://www.gao.gov/new.items/d07737.pdf> (last accessed January 21, 2022).

1 70. When cyber criminals access financial information and other personally sensitive
 2 data—as they did here—there is no limit to the amount of fraud to which Defendant may have
 3 exposed Representative Plaintiff and Class Members.

4 71. And data breaches are preventable.⁸ As Lucy Thompson wrote in the DATA BREACH
 5 AND ENCRYPTION HANDBOOK, “[i]n almost all cases, the data breaches that occurred could have
 6 been prevented by proper planning and the correct design and implementation of appropriate
 7 security solutions.”⁹ She added that “[o]rganizations that collect, use, store, and share sensitive
 8 personal data must accept responsibility for protecting the information and ensuring that it is not
 9 compromised”¹⁰

10 72. Most of the reported data breaches are a result of lax security and the failure to
 11 create or enforce appropriate security policies, rules, and procedures . . . Appropriate information
 12 security controls, including encryption, must be implemented and enforced in a rigorous and
 13 disciplined manner so that a *data breach never occurs*.¹¹

14 73. Here, Defendant knew of the importance of safeguarding PII and financial
 15 information and of the foreseeable consequences that would occur if Representative Plaintiff’s and
 16 Class Members’ PII and financial information was stolen, including the significant costs that
 17 would be placed on Representative Plaintiff and Class Members as a result of a breach of this
 18 magnitude. As detailed above, Defendant are large, sophisticated organizations with the resources
 19 to deploy robust cybersecurity protocols. They knew, or should have known, that the development
 20 and use of such protocols were necessary to fulfill its statutory and common law duties to
 21 Representative Plaintiff and Class Members. Its failure to do so is, therefore, intentional, willful,
 22 reckless and/or grossly negligent.

23 74. Defendant disregarded the rights of Representative Plaintiff and Class Members by,
 24 *inter alia*, (i) intentionally, willfully, recklessly, or negligently failing to take adequate and
 25 reasonable measures to ensure that its network servers were protected against unauthorized

26 _____
 27 ⁸ Lucy L. Thompson, “Despite the Alarming Trends, Data Breaches Are Preventable,” *in*
 DATA BREACH AND ENCRYPTION HANDBOOK (Lucy Thompson, ed., 2012)

28 ⁹ *Id.* at 17.

¹⁰ *Id.* at 28.

¹¹ *Id.*

COLE & VAN NOTE
ATTORNEYS AT LAW
555 12TH STREET, SUITE 1725
OAKLAND, CA 94607
TEL: (510) 891-9800

1 intrusions; (ii) failing to disclose that they did not have adequately robust security protocols and
2 training practices in place to adequately safeguard Representative Plaintiff’s and Class Members’
3 PII and financial information; (iii) failing to take standard and reasonably available steps to prevent
4 the Data Breach; (iv) concealing the existence and extent of the Data Breach for an unreasonable
5 duration of time; and (v) failing to provide Representative Plaintiff and Class Members prompt
6 and accurate notice of the Data Breach.

7
8 **FIRST CLAIM FOR RELIEF**
9 **Negligence**
10 **(On behalf of the Nationwide Class and the California Subclass)**

11 75. Each and every allegation of the preceding paragraphs is incorporated in this cause
12 of action with the same force and effect as though fully set forth herein

13 76. At all times herein relevant, Defendant owed Representative Plaintiff and Class
14 Members a duty of care, *inter alia*, to act with reasonable care to secure and safeguard their PII
15 and financial information and to use commercially reasonable methods to do so. Defendant took
16 on this obligation upon accepting and storing the PII and financial information of Representative
17 Plaintiff and Class Members in its computer systems and on its networks.

- 18 77. Among these duties, Defendant were expected:
- 19 a. to exercise reasonable care in obtaining, retaining, securing, safeguarding,
20 deleting, and protecting the PII and financial information in its possession;
 - 21 b. to protect Representative Plaintiff’s and Class Members’ PII and financial
22 information using reasonable and adequate security procedures and systems
23 that were/are compliant with industry-standard practices;
 - 24 c. to implement processes to quickly detect the Data Breach and to timely act
25 on warnings about data breaches; and
 - 26 d. to promptly notify Representative Plaintiff and Class Members of any data
27 breach, security incident, or intrusion that affected or may have affected its
28 PII and financial information.

78. Defendant knew that the PII and financial information was private and confidential
and should be protected as private and confidential and, thus, Defendant owed a duty of care not

1 to subject Representative Plaintiff and Class Members to an unreasonable risk of harm because
 2 they were foreseeable and probable victims of any inadequate security practices.

3 79. Defendant knew, or should have known, of the risks inherent in collecting and
 4 storing PII and financial information, the vulnerabilities of its data security systems, and the
 5 importance of adequate security. Defendant knew about numerous, well-publicized data breaches.

6 80. Defendant knew, or should have known, that its data systems and networks did not
 7 adequately safeguard Representative Plaintiff's and Class Members' PII and financial information.

8 81. Only Defendant was in the position to ensure that its systems and protocols were
 9 sufficient to protect the PII and financial information that Representative Plaintiff and Class
 10 Members had entrusted to it.

11 82. Defendant breached its duties to Representative Plaintiff and Class Members by
 12 failing to provide fair, reasonable, or adequate computer systems and data security practices to
 13 safeguard the PII and financial information of Representative Plaintiff and Class Members.

14 83. Because Defendant knew that a breach of its systems could damage thousands of
 15 individuals, including Representative Plaintiff and Class Members, Defendant had a duty to
 16 adequately protect its data systems and the PII and financial information contained therein.

17 84. Representative Plaintiff's and Class Members' willingness to entrust Defendant
 18 with its PII and financial information was predicated on the understanding that Defendant would
 19 take adequate security precautions. Moreover, only Defendant had the ability to protect its systems
 20 and the PII and financial information they stored on them from attack. Thus, Defendant had a
 21 special relationship with Representative Plaintiff and Class Members.

22 85. Defendant also had independent duties under state and federal laws that required
 23 Defendant to reasonably safeguard Representative Plaintiff's and Class Members' PII and
 24 financial information and promptly notify them about the Data Breach. These "independent duties"
 25 are untethered to any contract between Defendant and Representative Plaintiff and/or the
 26 remaining Class Members.

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

COLE & VAN NOTE
ATTORNEYS AT LAW
555 12TH STREET, SUITE 1725
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

- a. by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard the PII and financial information of Representative Plaintiff and Class Members;
- b. by failing to timely and accurately disclose that Representative Plaintiff's and Class Members' PII and financial information had been improperly acquired or accessed;
- c. by failing to adequately protect and safeguard the PII and financial information by knowingly disregarding standard information security principles, despite obvious risks, and by allowing unmonitored and unrestricted access to unsecured PII and financial information;
- d. by failing to provide adequate supervision and oversight of the PII and financial information with which they were and are entrusted, in spite of the known risk and foreseeable likelihood of breach and misuse, which permitted an unknown third party to gather PII and financial information of Representative Plaintiff and Class Members, misuse the PII and intentionally disclose it to others without consent.
- e. by failing to adequately train its employees to not store PII and financial information longer than absolutely necessary;
- f. by failing to consistently enforce security policies aimed at protecting Representative Plaintiff's and the Class Members' PII and financial information;
- g. by failing to implement processes to quickly detect data breaches, security incidents, or intrusions; and
- h. by failing to encrypt Representative Plaintiff's and Class Members' PII and financial information and monitor user behavior and activity in order to identify possible threats.

87. Defendant's willful failure to abide by these duties was wrongful, reckless, and grossly negligent in light of the foreseeable risks and known threats.

88. As a proximate and foreseeable result of Defendant's grossly negligent conduct, Representative Plaintiff and Class Members have suffered damages and are at imminent risk of additional harms and damages (as alleged above).

89. The law further imposes an affirmative duty on Defendant to timely disclose the unauthorized access and theft of the PII and financial information to Representative Plaintiff and Class Members so that they could and/or still can take appropriate measures to mitigate damages, protect against adverse consequences and thwart future misuse of its PII and financial information.

COLE & VAN NOTE
ATTORNEYS AT LAW
555 12TH STREET, SUITE 1725
OAKLAND, CA 94607
TEL: (510) 891-9800

1 90. Defendant breached its duty to notify Representative Plaintiff and Class Members
2 of the unauthorized access by waiting months after learning of the Data Breach to notify
3 Representative Plaintiff and Class Members and then by failing and continuing to fail to provide
4 Representative Plaintiff and Class Members sufficient information regarding the breach. To date,
5 Defendant has not provided sufficient information to Representative Plaintiff and Class Members
6 regarding the extent of the unauthorized access and continues to breach its disclosure obligations
7 to Representative Plaintiff and Class Members.

8 91. Further, through its failure to provide timely and clear notification of the Data
9 Breach to Representative Plaintiff and Class Members, Defendant prevented Representative
10 Plaintiff and Class Members from taking meaningful, proactive steps to secure its PII and financial
11 information, and to access its medical records and histories.

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

19 93. Defendant's wrongful actions, inactions, and omissions constituted (and continue
20 to constitute) common law negligence.

21 94. The damages Representative Plaintiff and Class Members have suffered (as alleged
22 above) and will suffer, were and are the direct and proximate result of Defendant's grossly
23 negligent conduct.

24 95. Additionally, 15 U.S.C. §45 (FTC Act, Section 5) prohibits "unfair . . . practices in
25 or affecting commerce," including, as interpreted, and enforced by the FTC, the unfair act or
26 practice by businesses, such as Defendant, of failing to use reasonable measures to protect PII and
27 financial information. The FTC publications and orders described above also form part of the basis
28 of Defendant's duty in this regard.

COLE & VAN NOTE
ATTORNEYS AT LAW
555 12TH STREET, SUITE 1725
OAKLAND, CA 94607
TEL: (510) 891-9800

1 96. Defendant violated 15 U.S.C. § 45 by failing to use reasonable measures to protect
2 PII and financial information and not complying with applicable industry standards, as described
3 in detail herein. Defendant's conduct was particularly unreasonable given the nature and amount
4 of PII and financial information it obtained and stored and the foreseeable consequences of the
5 immense damages that would result to Representative Plaintiff and Class Members.

6 97. Defendant's violation of 15 U.S.C. § 45 constitutes negligence *per se*. Defendant
7 also violated the HIPAA Privacy and Security rules which, likewise, constitutes negligence *per se*.

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

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

1 appropriation, disclosure, encumbrance, exfiltration, release, theft, use, and/or viewing, such as
 2 following basic principles of protecting its networks and data systems.

3 106. Defendant voluntarily received, in confidence, Representative Plaintiff's and Class
 4 Members' PII and financial information with the understanding that the PII and financial
 5 information would not be accessed by, acquired by, appropriated by, disclosed to, encumbered by,
 6 exfiltrated by, released to, stolen by, used by and/or viewed by the public or any unauthorized
 7 third-parties.

8 107. Due to Defendant's failure to prevent, detect, and avoid the Data Breach from
 9 occurring by, *inter alia*, not following best information security practices to secure Representative
 10 Plaintiff's and Class Members' PII and financial information, Representative Plaintiff's and Class
 11 Members' PII and financial information was accessed by, acquired by, appropriated by, disclosed
 12 to, encumbered by, exfiltrated by, released to, stolen by, used by and/or viewed by unauthorized
 13 third-parties beyond Representative Plaintiff's and Class Members' confidence, and without their
 14 express permission.

15 108. As a direct and proximate cause of Defendant's actions and/or omissions,
 16 Representative Plaintiff and Class Members have suffered damages, as alleged therein.

17 109. But for Defendant's failure to maintain and protect Representative Plaintiff's and
 18 Class Members' PII and financial information in violation of the parties' understanding of
 19 confidence, its PII and financial information would not have been accessed by, acquired by,
 20 appropriated by, disclosed to, encumbered by, exfiltrated by, released to, stolen by, used by and/or
 21 viewed by unauthorized third-parties. The Data Breach was the direct and legal cause of the misuse
 22 of Representative Plaintiff's and Class Members' PII and financial information, as well as the
 23 resulting damages.

24 110. The injury and harm Representative Plaintiff and Class Members suffered and will
 25 continue to suffer was the reasonably foreseeable result of Defendant's unauthorized misuse of
 26 Representative Plaintiff's and Class Members' PII and financial information. Defendant knew its
 27 data systems and protocols for accepting and securing Representative Plaintiff's and Class
 28

COLE & VAN NOTE
ATTORNEYS AT LAW
555 12TH STREET, SUITE 1725
OAKLAND, CA 94607
TEL: (510) 891-9800

1 Members' PII and financial information had security and other vulnerabilities that placed
2 Representative Plaintiff's and Class Members' PII and financial information in jeopardy.

3 111. As a direct and proximate result of Defendant's breaches of confidence,
4 Representative Plaintiff and Class Members have suffered and will suffer injury, as alleged herein,
5 including, but not limited to, (a) actual identity theft; (b) the compromise, publication, and/or theft
6 of its PII and financial information; (c) out-of-pocket expenses associated with the prevention,
7 detection, and recovery from identity theft and/or unauthorized use of its PII and financial
8 information; (d) lost opportunity costs associated with effort expended and the loss of productivity
9 addressing and attempting to mitigate the actual and future consequences of the Data Breach,
10 including but not limited to, efforts spent researching how to prevent, detect, contest, and recover
11 from identity theft; (e) the continued risk to its PII and financial information, which remains in
12 Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fail
13 to undertake appropriate and adequate measures to protect Class Members' PII and financial
14 information in its continued possession; (f) future costs in terms of time, effort, and money that
15 will be expended as result of the Data Breach for the remainder of the lives of Representative
16 Plaintiff and Class Members; (g) the diminished value of Representative Plaintiff's and Class
17 Members' PII and financial information; and (h) the diminished value of Defendant's services for
18 which Representative Plaintiff and Class Members paid and received.

19
20 **THIRD CLAIM FOR RELIEF**
21 **Breach of Implied Contract**
22 **(On behalf of the Nationwide Class and the California Subclass)**

23 112. Each and every allegation of the preceding paragraphs is incorporated in this cause
24 of action with the same force and effect as though fully set forth therein.

25 113. Through its course of conduct, Defendant, Representative Plaintiff and Class
26 Members entered into implied contracts for Defendant to implement data security adequate to
27 safeguard and protect the privacy of Representative Plaintiff's and Class Members' PII and
28 financial information.

COLE & VAN NOTE
ATTORNEYS AT LAW
555 12TH STREET, SUITE 1725
OAKLAND, CA 94607
TEL: (510) 891-9800

1 114. Defendant required Representative Plaintiff and Class Members to provide and
2 entrust their PII and financial information as a condition of obtaining Defendant’s services.

3 115. Defendant solicited and invited Representative Plaintiff and Class Members to
4 provide their PII and financial information as part of Defendant’s regular business practices.
5 Representative Plaintiff and Class Members accepted Defendant’s offers and provided their PII
6 and financial information to Defendant.

7 116. As a condition of being direct customers of Defendant, Representative Plaintiff and
8 Class Members provided and entrusted their PII and financial information to Defendant. In so
9 doing, Representative Plaintiff and Class Members entered into implied contracts with Defendant
10 by which Defendant agreed to safeguard and protect such non-public information, to keep such
11 information secure and confidential, and to timely and accurately notify Representative Plaintiff
12 and Class Members if its data had been breached and compromised or stolen.

13 117. A meeting of the minds occurred when Representative Plaintiff and Class Members
14 agreed to, and did, provide their PII and financial information to Defendant, in exchange for,
15 amongst other things, the protection of their PII and financial information.

16 118. Representative Plaintiff and Class Members fully performed their obligations under
17 the implied contracts with Defendant.

18 119. Defendant breached the implied contracts it made with Representative Plaintiff and
19 Class Members by failing to safeguard and protect its PII and financial information and by failing
20 to provide timely and accurate notice to them that their PII and financial information was
21 compromised as a result of the Data Breach.

22 120. As a direct and proximate result of Defendant’s above-described breach of implied
23 contract, Representative Plaintiff and Class Members have suffered (and will continue to suffer)
24 (a) ongoing, imminent, and impending threat of identity theft crimes, fraud, and abuse, resulting
25 in monetary loss and economic harm; (b) actual identity theft crimes, fraud, and abuse, resulting
26 in monetary loss and economic harm; (c) loss of the confidentiality of the stolen confidential data;
27 (d) the illegal sale of the compromised data on the dark web; (e) lost work time; and (f) other
28 economic and non-economic harm.

FOURTH CLAIM FOR RELIEF

**Breach of the Implied Covenant of Good Faith and Fair Dealing
(On behalf of the Nationwide Class and the California Subclass)**

121. Each and every allegation of the preceding paragraphs is incorporated in this cause of action with the same force and effect as though fully set forth therein.

122. Every contract in this state has an implied covenant of good faith and fair dealing. This implied covenant is an independent duty and may be breached even when there is no breach of a contract’s actual and/or express terms.

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

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

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

RELIEF SOUGHT

WHEREFORE, Representative Plaintiff, on behalf of herself and each member of the proposed National Class and the California Subclass, respectfully request that the Court enter judgment in their favor and for the following specific relief against Defendant as follows:

1. That the Court declare, adjudge, and decree that this action is a proper class action and certify each of the proposed classes and/or any other appropriate subclasses under F.R.C.P. Rule 23 (b)(1), (b)(2), and/or (b)(3), including appointment of Representative Plaintiff’s counsel as Class Counsel;

COLE & VAN NOTE
ATTORNEYS AT LAW
555 12TH STREET, SUITE 1725
OAKLAND, CA 94607
TEL: (510) 891-9800

COLE & VAN NOTE
ATTORNEYS AT LAW
555 12TH STREET, SUITE 1725
OAKLAND, CA 94607
TEL: (510) 891-9800

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

3 3. That the Court enjoin Defendant, ordering them to cease and desist from unlawful
4 activities;

5 4. For equitable relief enjoining Defendant from engaging in the wrongful conduct
6 complained of herein pertaining to the misuse and/or disclosure of Representative Plaintiff's and
7 Class Members' PII, and from refusing to issue prompt, complete, any accurate disclosures to
8 Representative Plaintiff and Class Members;

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

12 a. prohibiting Defendant from engaging in the wrongful and unlawful acts
13 described herein;

14 b. requiring Defendant to protect, including through encryption, all data
15 collected through the course of business in accordance with all applicable
16 regulations, industry standards, and federal, state, or local laws;

17 c. requiring Defendant to delete and purge the PII of Representative Plaintiff
18 and Class Members unless Defendant can provide to the Court reasonable
19 justification for the retention and use of such information when weighed
20 against the privacy interests of Representative Plaintiff and Class Members;

21 d. requiring Defendant to implement and maintain a comprehensive
22 Information Security Program designed to protect the confidentiality and
23 integrity of Representative Plaintiff's and Class Members' PII;

24 e. requiring Defendant to engage independent third-party security auditors and
25 internal personnel to run automated security monitoring, simulated attacks,
26 penetration tests, and audits on Defendant's systems on a periodic basis;

27 f. prohibiting Defendant from maintaining Representative Plaintiff's and
28 Class Members' PII on a cloud-based database;

 g. requiring Defendant to segment data by creating firewalls and access
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

COLE & VAN NOTE
ATTORNEYS AT LAW
555 12TH STREET, SUITE 1725
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

employees' respective responsibilities with handling PII, as well as protecting the PII 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 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;

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;
- 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 Classes(es) and/or Subclass(es), hereby demands a trial by jury for all issues triable by jury.

Dated: November 16, 2022

COLE & VAN NOTE

By: /s/ Scott Edward Cole
Scott Edward Cole, Esq.
Attorneys for Representative Plaintiff
and the Plaintiff Classes