Scott Edward Cole, Esq. (S.B. #160744)
Alicyn B. Whitley, Esq. (S.B. #325927)
COLE & VAN NOTE
555 12th Street, Suite 2100
Oakland, California 94607
Telephone: (510) 891-9800
Facsimile: (510) 891-7030
Email: sec@colevannote.com
Email: abw@colevannote.com

M. Anderson Berry, Esq. (S.B. #262879)
Gregory Haroutunian, Esq. (S.B. #330263)
CLAYEO C. ARNOLD
A PROFESSIONAL CORPORATION
865 Howe Avenue
Sacramento, CA 95825
Telephone: (916) 239-4778
Facsimile: (916) 924-1829
Email: aberry@justice4you.com
Email: gharoutunian@justice4you.com

Robert C. Schubert, Esq. (S.B. #62684)
Amber L. Schubert, Esq. (S.B. #278696)
SCHUBERT JONCKHEER & KOLBE LLP
2001 Union Street, Suite 200
San Francisco, CA 94123
Telephone: (415) 788-4220
Facsimile: (415) 788-0161
Email: rschubert@sjk.law
Email: aschubert@sjk.law

Interim Co-Lead Class Counsel

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

IN THE SUPERIOR COURT OF THE STATE OF CALIFORNIA

IN AND FOR THE COUNTY OF ALAMEDA

IN RE: PATELCO CREDIT UNION DATA SECURITY LITIGATION

Case No. 24CV082095

CLASS ACTION

CONSOLIDATED CLASS ACTION COMPLAINT FOR DAMAGES, INJUNCTIVE AND EQUITABLE RELIEF FOR:

1. **NEGLIGENCE;**
2. **BREACH OF IMPLIED CONTRACT;**
3. **BREACH OF THE IMPLIED COVENANT OF GOOD FAITH AND FAIR DEALING;**
4. **VIOLATIONS OF THE UNFAIR COMPETITION LAW (CAL. BUS. & PROF. CODE §§ 17200, *ET SEQ.*);**
5. **VIOLATIONS OF THE CALIFORNIA CONSUMER PRIVACY ACT OF 2018, (CAL. CIV. CODE §§ 1798.100, *ET SEQ.*);**
6. **VIOLATIONS OF THE CALIFORNIA CUSTOMER RECORDS ACT (CAL. CIV. CODE §§ 1798.80, *ET SEQ.*).**

Assigned for All Purposes to:
Hon. Michael Markman; Dept. 23

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

INTRODUCTION

1. Representative Plaintiffs Anand Chaudhry, Jamie Wallace, Joshua Warren, Carl Cordell, Austin Lawhead, Bradley Tanzman, Darren Van Antwerp, Darrel Adams, Wily Lee, Siobhan Gallagher, Sean McGinity and Daniel Corona ("Plaintiffs" or "Representative Plaintiffs") bring this class action against Patelco Credit Union ("Defendant" or "Patelco") for its failure to properly secure and safeguard Representative Plaintiffs' and/or Class Members' personally identifiable information stored within Defendant's information network. All such information is hereafter referred to in the aggregate as "Private Information" or "PII".[1]

2. In connection with Defendant providing services to its members, customers provided Defendant with their sensitive PII, including names, dates of birth, addresses, Social Security numbers, driver's license numbers and financial account information.

3. With this action, Representative Plaintiffs seek to hold Defendant responsible for the harms it caused and will continue to cause Representative Plaintiffs and, at least, 1,009,472[2] other similarly situated persons in the massive and preventable cyberattack purportedly discovered by Defendant on June 29, 2024, by which cybercriminals infiltrated Defendant's inadequately protected network and accessed the Private Information (the "Data Breach").

4. While Defendant claims to have discovered the breach as early as June 29, 2024, Defendant did not provide specific, individual notice of the Data Breach to Plaintiffs and Class Members until August 20, 2024, when it sent a Notice of Data Breach via email informing Plaintiffs and Class Members that their PII was "accessed" during the breach. However, this notice

---

[1] Personally identifiable information ("PII") generally incorporates information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information. 2 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 identifiers that do not on their face name an individual, but that are considered to be particularly sensitive and/or valuable if in the wrong hands (for example, Social Security numbers, passport numbers, driver's license numbers, financial account numbers, etc.).

[2] https://www.maine.gov/agviewer/content/ag/985235c7-cb95-4be2-8792-a1252b4f8318/75619fc1-b3ca-440d-85e3-4367b1017ea3.html (last accessed, Oct. 1, 2024).

failed to specify exactly what pieces of Plaintiffs' PII had been stolen by cybercriminals, simply noting "the specific data that was accessed has not been determined."[3]

5. Further, the notices Defendant posted on its website obscured the nature of the cyberattack and threat it posed—failing to adequately inform Representative Plaintiffs and Class Members of how many people were impacted, how the cybercriminal remotely accessed its systems, whether the exfiltrated information was encrypted or anonymized, or what specific remedial steps Defendant took to safeguard PII within its systems and networks (or otherwise purge unnecessary information) to prevent further cyberattacks going forward. All that Defendant provided were vague assurances that "[w]e remain committed to making strategic investments in the advanced tools, teams, and partners that help strengthen our security measures."[4]

6. As a result of the Data Breach, Defendant shut down some of its day-to-day banking systems, including online banking, its mobile app, and its call center. Accordingly, important services, such as transfers (including Zelle), direct deposit, balance inquiries and payments became unavailable. It also limited debit and credit card transactions.[5]

7. The Data Breach was directly and proximately caused by Defendant's failure to implement reasonable and industry standard data security practices necessary to protect its systems from a foreseeable and preventable cyberattack. Defendant acquired, collected and stored Representative Plaintiffs' and Class Members' Private Information. Therefore, at all relevant times, Defendant knew or should have known that Representative Plaintiffs and Class Members would use Defendant's services to store and/or share sensitive data, including highly confidential Private Information.

8. Defendant disregarded the rights of Representative Plaintiffs and Class Members by intentionally, willfully, recklessly and/or negligently failing to take and implement adequate and reasonable measures to ensure that Representative Plaintiffs' and Class Members' Private

---

[3] Notice of Data Breach, PATELCO CREDIT UNION (August 20, 2024), https://www.patelco.org/notification.

[4] Security Incident Updates & Information Center, PATELCO CREDIT UNION, https://www.patelco.org/securityupdate#qa (last visited Oct. 2, 2024).

[5] *Security Incident Updates & Information Center,* PATELCO CREDIT UNION, https://www.patelco.org/about-patelco/who-we-are (last visited Oct. 2, 2024).

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

Information was safeguarded, failing to take available steps to prevent an unauthorized disclosure of data, and failing to follow applicable, required and appropriate protocols, policies and procedures regarding the encryption of data, even for internal use. As a result, Representative Plaintiffs' and Class Members' Private Information was compromised through disclosure to an unknown and unauthorized third party—an undoubtedly nefarious third party seeking to profit off this disclosure by defrauding Representative Plaintiffs and Class Members in the future. Representative Plaintiffs and Class Members have a continuing interest in ensuring their information is and remains safe and are entitled to injunctive and other equitable relief.

JURISDICTION AND VENUE

9. This Court has jurisdiction over Representative Plaintiffs' and Class Members' claims for damages and injunctive relief pursuant to, *inter alia*, California's Consumer Privacy Act (Cal. Civ. Code §§ 1798.100, *et seq.*), California's Customer Records Act (Cal. Civ. Code §§ 1798.80, *et seq.*), California's Unfair Competition Law (Cal. Bus. & Prof. Code §§ 17200, *et seq.*), among other California state statutes.

10. This Court has original jurisdiction over this action pursuant to Cal. Code Civ. Proc. § 410.10 because Defendant has sufficient minimum contacts with California and/or Defendant otherwise purposely avails itself of the markets in California. The acts at issue in this complaint occurred in California, Plaintiffs are citizens of California, and Defendant conducts substantial business, including the promotion, marketing and sale of its services in California. These acts render the exercise of jurisdiction by this Court permissible under traditional notions of fair play and substantial justice.

11. Venue as to Defendant is proper in this judicial district pursuant to California Code of Civil Procedure § 395(a). Defendant is headquartered in, operates in, and employs and transacts business with numerous Class Members within this County and transacts business, has agents and is otherwise within this Court's jurisdiction for purposes of service of process. The unlawful acts alleged herein have had a direct effect on Representative Plaintiffs and those similarly situated within the State of California and within this County.

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

PLAINTIFFS

Plaintiff Anand Chaudhry

12. Plaintiff Anand Chaudhry is an adult individual and, at all relevant times herein, was a resident and citizen of the State of California. Plaintiff is a victim of the Data Breach.

13. Defendant received highly sensitive Private Information from Chaudhry in connection with the services he obtained. As a result, Chaudhry's information was among the data accessed by an unauthorized third party in the Data Breach.

14. At all times herein relevant, Representative Plaintiff Chaudhry is and was a member of the Class(es).

15. Chaudhry's Private Information was exposed in the Data Breach because Defendant stored and/or shared Chaudhry's Private Information. Representative Plaintiff Chaudhry's Private Information was within the possession and control of Defendant at the time of the Data Breach.

16. In addition, Chaudhry is the owner and operator of a private chiropractic practice whose business was deleteriously affected by service disruptions at Patelco because the finances for his business were primarily handled by Patelco at the time of the Data Breach. During the more than two-week period in which Patelco shut down online banking services, Chaudhry could not accept payments from his patients as usual because he had set up payments from his patients to go to his Patelco account. Thus, to cover the daily expenses of his business, during this same two-week period, Chaudhry traveled by car every day to a Patelco bank branch to withdraw $500 (the maximum Patelco was allowing during this time period). On some days, Chaudhry even went to two separate Patelco bank branches in a single day to withdraw $500 from each branch in order to cover necessary business expenses. Chaudhry emphasized that each branch visit could last from 30 minutes to an hour due to the long lines during the period when online services were shut down, causing him to spend significant time off work just to access the funds necessary to run his private practice. Chaudhry estimates he used about a quarter of a tank of gas per day just traveling to and from his private practice to Patelco bank branches.

17. However, the service disruption at Patelco not only deleteriously affected Chaudhry's professional life, but his personal life as well. Because Patelco had shut down online banking services for over two weeks, Chaudhry could not access his checking or savings account online, and he was, thus, was unable to pay his rent and mortgage in a timely manner. Eventually, Chaudhry was forced to open a credit card account at a new bank in order just to "continue functioning," which caused him to accrue debt with interest he otherwise would not have accrued but for the service disruptions at Patelco.

18. In addition, Chaudhry did not receive personal notice that a Data Breach had occurred at Patelco until August 20, 2024, even though Patelco became aware of the breach in or around June 29, 2024. This delay in notification caused Chaudhry harm that was separate and independent from the harms caused by the Data Breach itself because the delay prevented Chaudhry from mitigating his own damages in a timely manner.

19. Furthermore, after learning of the Data Breach, Chaudhry spent $250 purchasing LifeLock, an identity theft protection service, in order to protect himself from hackers on the Dark Web who now have access to Chaudhry's PII due to the Data Breach.

20. Thus, Chaudhry spent time dealing with the consequences of the Data Breach, which included and continues to include, time spent verifying the legitimacy and impact of the Data Breach, exploring credit monitoring and identity theft insurance options, self-monitoring his accounts and seeking legal counsel regarding his options for remedying and/or mitigating the effects of the Data Breach. This time has been lost forever and cannot be recaptured.

21. Chaudhry suffered actual injury in the form of damages to and diminution in the value of his Private Information—a form of intangible property that Plaintiff entrusted to Defendant, which was compromised in and as a result of the Data Breach.

22. Chaudhry suffered lost time, annoyance, interference and inconvenience as a result of the Data Breach and has anxiety and increased concerns for the loss of privacy, as well as anxiety over the impact of cybercriminals accessing, using and selling his Private Information.

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

23. Chaudhry suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft and misuse resulting from his Private Information being placed in the hands of unauthorized third parties/criminals.

24. Chaudhry has a continuing interest in ensuring that his Private Information, which, upon information and belief, remains in Defendant's possession, is protected and safeguarded from future breaches.

Plaintiff Jamie Wallace

25. Plaintiff Jamie Wallace is an adult individual and, at all relevant times herein, was a resident and citizen of the State of California. Wallace is a victim of the Data Breach.

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

27. At all times herein relevant, Representative Plaintiff Wallace is and was a member of the Class(es).

28. Wallace's Private Information was exposed in the Data Breach because Defendant stored and/or shared Wallace's Private Information. Representative Plaintiff Wallace's Private Information was within the possession and control of Defendant at the time of the Data Breach.

29. Wallace did not receive personal notice that a Data Breach had occurred at Patelco until August 20, 2024, even though Patelco had knowledge of the Data Breach since at least June 29, 2024. This delay in notification caused harm to Wallace independent of the harms caused by the Data Breach itself because the delay prevented Wallace from mitigating her own damages in a timely manner.

30. Since May 23, 2024, (the date that Patelco acknowledges that hackers first gained unauthorized access to their databases), Wallace has experienced alarming instances of identity theft and fraud. For example, since the Data Breach, two separate accounts have been fraudulently opened in Wallace's names—one for a Discover card and another at Citibank. In addition, since the Data Breach it appears someone has also hacked into Wallace's account with CarMax, (a used car retailer), as CarMax claims several payments to it from Wallace have been reversed even

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

though the bank account linked to Wallace's CarMax account has documentation showing that the bank sent the payments to CarMax. As a result, CarMax is claiming Wallace owes it $1,400 and charged Wallace a late fee of $117, both of which Wallace is currently contesting.

31. Apart from having to deal with identity theft and fraudulent transactions, Wallace also reports experiencing a significant uptick in spam calls, emails and texts since May 23, 2024. Specifically, Wallace has received a total of 350 spam calls, emails, and text messages since the Data Breach, and she believes and alleges this was directly caused by the Data Breach because she did not have a problem with spam before May 23, 2024.

32. Furthermore, according to credit monitoring services used by Wallace, her name, Social Security number, date of birth, email address and home address have all been found on the Dark Web since the Data Breach—exposing Wallace to even more potential instances of identity theft and fraud in the future.

33. Wallace also experienced strife in her personal life due to the shutdown of online banking services at Patelco, which lasted from June 28, 2024 to July 15, 2024. During this period, Wallace was forced to travel over 30 miles to her nearest Patelco bank branch office to withdraw the cash she needed to order to cover her necessary daily expenses—or otherwise she had to withdraw cash from an ATM and pay the accompanying convenience fee for using a non-Patelco ATM, as she had no online access to her checking or savings accounts with Patelco. Wallace estimates that traveling to Patelco bank branches or ATMs has cost her $510 as she had to fill her gas tank 7 times in order to travel to these locations. Furthermore, because of her inability to access her financial accounts with Patelco, Wallace was forced to borrow money and food from friends in order to feed her family.

34. In total, Wallace estimates she has spent over 98 hours monitoring her accounts for fraud, contesting fraudulent transactions and traveling to Patelco branches to withdraw the cash necessary for her daily expenses.

35. Thus, Wallace spent time dealing with the consequences of the Data Breach, which included and continues to include, time spent verifying the legitimacy and impact of the Data Breach, exploring credit monitoring and identity theft insurance options, self-monitoring her

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

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

36. Wallace suffered actual injury in the form of damages to and diminution in the value of her Private Information—a form of intangible property that Plaintiff entrusted to Defendant, which was compromised in and as a result of the Data Breach.

37. Wallace suffered lost time, annoyance, interference and inconvenience as a result of the Data Breach and has anxiety and increased concerns for the loss of privacy, as well as anxiety over the impact of cybercriminals accessing, using and selling his Private Information.

38. Wallace suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft and misuse resulting from his Private Information being placed in the hands of unauthorized third parties/criminals.

39. Wallace has a continuing interest in ensuring that her Private Information, which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future breaches.

Plaintiff Joshua Warren

40. Plaintiff Joshua Warren is an adult individual and, at all relevant times herein, was a resident and citizen of the State of California. Warren is a victim of the Data Breach.

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

42. At all times herein relevant, Representative Plaintiff Warren is and was a member of the Class(es).

43. Warren's Private Information was exposed in the Data Breach because Defendant stored and/or shared Warren's Private Information. Representative Plaintiff Warren's Private Information was within the possession and control of Defendant at the time of the Data Breach.

44. Warren did not receive personal notice that his PII was exposed in the Data Breach until August 20, 2024, even though Patelco became aware of the Data Breach on June 29, 2024.

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

This delay in notification was harmful in itself because it prevented Warren from mitigating his own damages in a timely manner.

45. Furthermore, in approximately early June, Warren discovered a fraudulent charge on his credit card linked to a non-Patelco account. Warren believes and alleges this fraudulent charge is linked to the Data Breach due to the timing, considering the fact that hackers first gained access to Patelco's computer systems on May 23, 2024.

46. Disconcertingly, Warren has also received at least 3 alerts from various credit monitoring services he uses, notifying him that his PII has been found on the Dark Web. Subsequently, he experienced an incident of identity theft. Specifically, someone attempted to fraudulently open a sports-booking account in Warren's name.

47. In addition, Warren also experienced a surge of spam calls, texts and emails immediately following the Data Breach, which he describes as "a ton." Warren believes and alleges this surge in vexatious spamming was directly caused by the Data Breach because he used a separate email to sign up for a Patelco account, and the spam emails he is receiving are all coming to the email associated with his Patelco account.

48. In addition to instances of identity theft and fraud, Warren also experienced many service disruptions in his access to his Patelco financial accounts due to the Data Breach. When Patelco shut down all of its online financial services between June 28, 2024 and July 15, 2024, Warren was unable to access his checking or savings accounts online and was unable to use his credit card. Even more disconcertingly, Warren could not access the monthly paycheck he usually receives from his employer.

49. This disruption in services also led to missed opportunities for Warren. For example, Warren missed an opportunity to invest in cryptocurrency during a dip in the cryptocurrency market because he was unable to access his online financial accounts with Patelco. Furthermore, Warren was unable to hire a contractor to do the siding on his house during the summer months like he had originally planned because he could not access his online financial accounts with Patelco.

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

50. Finally, aside from the more tangible harms described above, Warren also reports that the Data Breach has caused him "intense" feelings of fear and anxiety when Patelco's online banking services were shut down as he was worried about the security of his savings and his ability to pay his mortgage.

51. Thus, Warren spent time dealing with the consequences of the Data Breach, which included and continues to include time spent verifying the legitimacy and impact of the Data Breach, exploring credit monitoring and identity theft insurance options, self-monitoring his accounts and seeking legal counsel regarding his options for remedying and/or mitigating the effects of the Data Breach. This time has been lost forever and cannot be recaptured.

52. Warren suffered actual injury in the form of damages to and diminution in the value of his Private Information—a form of intangible property that he entrusted to Defendant, which was compromised in and as a result of the Data Breach.

53. Warren suffered lost time, annoyance, interference and inconvenience as a result of the Data Breach and has anxiety and increased concerns for the loss of privacy, as well as anxiety over the impact of cybercriminals accessing, using and selling his Private Information.

54. Warren suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft and misuse resulting from his Private Information being placed in the hands of unauthorized third parties and criminals.

55. Warren has a continuing interest in ensuring that his Private Information, which, upon information and belief, remains in Defendant's possession, is protected and safeguarded from future breaches.

Plaintiff Carl Cordell

56. Plaintiff Carl Cordell is an adult individual and, at all relevant times herein, was a resident and citizen of the State of California. Cordell is a victim of the Data Breach.

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

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

58. At all times herein relevant, Representative Plaintiff Cordell is and was a member of the Class(es).

59. Cordell's Private Information was exposed in the Data Breach because Defendant stored and/or shared Cordell's Private Information. Plaintiff Cordell's Private Information was within the possession and control of Defendant at the time of the Data Breach.

60. Although Patelco became aware of the Data Breach on June 29, 2024, Cordell did not receive a personal notice of the breach from Patelco until August 20, 2024. This delay in notification was harmful in itself because it prevented Cordell from mitigating his own damages in a timely manner.

61. To make matters even worse, Cordell has experienced fraud as a result of the Data Breach. Specifically, Cordell experienced hackers gaining access to, and making unauthorized charges on, his Instacart account shortly after the Data Breach occurred.

62. Furthermore, since May 23, 2024 (the date Patelco alleges hackers first gained access to its computer systems), Cordell has experienced a significant uptick in spam calls, texts and emails. This has led Cordell to believe that at least his name, phone number and address have been posted on the Dark Web as a result of the Data Beach.

63. In addition, Cordell experienced a debilitating disruption in his ability to access Patelco's financial services for over two weeks when Patelco shut down online banking services from June 29, 2024 to July 15, 2024. As a result, Cordell was unable to access his online Patelco account or mobile banking app which, in turn, prevented him from making credit or debit card payments for this entire period. Cordell reports this prevented him from paying his usual bills in a timely manner and, as a result, he spent a day getting a new bank account and closing his account with Patelco.

64. Consequently, the Data Breach has caused Cordell significant anxiety, stating "I feel like I will lose everything," and furthermore that he now has "no faith in banks."

65. Thus, Cordell spent time dealing with the consequences of the Data Breach, which included and continues to include, time spent verifying the legitimacy and impact of the Data Breach, exploring credit monitoring and identity theft insurance options, self-monitoring his

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

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

66. Cordell suffered actual injury in the form of damages to and diminution in the value of his Private Information—a form of intangible property that Plaintiff entrusted to Defendant, which was compromised in and as a result of the Data Breach.

67. Cordell suffered lost time, annoyance, interference and inconvenience as a result of the Data Breach and has anxiety and increased concerns for the loss of privacy, as well as anxiety over the impact of cybercriminals accessing, using and selling his Private Information.

68. Cordell suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft and misuse resulting from his Private Information being placed in the hands of unauthorized third parties/criminals.

69. Cordell has a continuing interest in ensuring that his Private Information, which, upon information and belief, remains in Defendant's possession, is protected and safeguarded from future breaches.

Plaintiff Austin Lawhead

70. Plaintiff Austin Lawhead is an adult individual and, at all relevant times herein, was a resident and citizen of the State of Oregon. Lawhead is a victim of the Data Breach.

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

72. At all times herein relevant, Plaintiff Lawhead is and was a member of the Class(es).

73. Lawhead's Private Information was exposed in the Data Breach because Defendant stored and/or shared Lawhead's Private Information. Plaintiff Lawhead's Private Information was within the possession and control of Defendant at the time of the Data Breach.

74. Lawhead did not receive personal notice that there had been a Data Breach at Patelco until August 20, 2024, despite the fact that Patelco became aware of the breach in or around June 29, 2024. Patelco has not explained its reasons for delaying notification, and this delay caused

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

Lawhead harm that was distinct and independent of the harm of the Data Breach itself because he was prevented from mitigating his own damages in a timely manner.

75. Additionally, as a result of the Data Breach, Lawhead lost access to his Patelco financial accounts for over two weeks when Patelco shutdown all online banking services from June 28, 2024 to July 15, 2024. During this period Lawhead reports he could not access his checking or savings account with Patelco. As a result, Lawhead was forced to live off his credit card for over two weeks in order to cover his necessary expenses, which incurred debt with interest. Lawhead was also forced to borrow money from a 401K account to cover his necessary expenses during the same time period due to his inability to access his Patelco financial accounts. Lawhead reports the experience of the Data Breach and being unable to access his Patelco financial accounts was very distressing, especially considering the fact that he had a toddler to look after.

76. Thus, Lawhead spent time dealing with the consequences of the Data Breach, which included and continues to include, time spent verifying the legitimacy and impact of the Data Breach, exploring credit monitoring and identity theft insurance options, self-monitoring his accounts, and seeking legal counsel regarding his options for remedying and/or mitigating the effects of the Data Breach. This time has been lost forever and cannot be recaptured.

77. Lawhead suffered actual injury in the form of damages to and diminution in the value of his Private Information—a form of intangible property that Plaintiff entrusted to Defendant, which was compromised in and as a result of the Data Breach.

78. Lawhead suffered lost time, annoyance, interference and inconvenience as a result of the Data Breach and has anxiety and increased concerns for the loss of privacy, as well as anxiety over the impact of cybercriminals accessing, using and selling his Private Information.

79. Lawhead suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft and misuse resulting from his Private Information being placed in the hands of unauthorized third parties and criminals.

80. Lawhead has a continuing interest in ensuring that his Private Information, which, upon information and belief, remains in Defendant's possession, is protected and safeguarded from future breaches.

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

Plaintiff Bradley Tanzman

81. Plaintiff Tanzman is an adult individual and, at all relevant times herein, was a resident and citizen of the State of California. Tanzman is a victim of the Data Breach.

82. Plaintiff Tanzman has been a Patelco member since the 1990s and, after leaving the credit union, returned as a member in approximately 2015.

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

84. At all times herein relevant, Tanzman is and was a member of the Class(es).

85. Tanzman's Private Information was exposed in the Data Breach because Defendant stored and/or shared Tanzman's Private Information. Tanzman's Private Information was within the possession and control of Defendant at the time of the Data Breach.

86. As a proximate result of the Data Breach, Plaintiff Tanzman suffered from not having access to his financial accounts and online banking services. Plaintiff Tanzman uses the Patelco mobile app to lock and unlock his ATM debit card. When the Data Breach occurred, Patelco shut down its app and online banking services, leaving Plaintiff Tanzman with no method to unlock his debit card. Thus, Plaintiff Tanzman was forced to wait in line at Patelco branch offices each day to withdraw cash. For sixteen straight days, Plaintiff Tanzman was forced to visit Patelco branch offices and wait in long lines to withdraw cash. During those visits, Patelco employees recorded his transactions on paper because the company's computer systems were inaccessible. As a result, Plaintiff Tanzman's account balances do not accurately reflect the transactions he made in branch offices.

87. Moreover, because cash withdrawals are limited to $500 per branch per day, Plaintiff Tanzman sometimes travels to multiple Patelco branch offices in a given day to withdraw sufficient cash. He spends significant time each day (at least an hour) simply travelling to and from Patelco branches. Plaintiff Tanzman also needed to acquire a cashier's check as payment to move into a new rental apartment but could not do so because Patelco's services were offline as a result

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

of the Data Breach. He has concerns for his personal financial security as a result of the Data Breach.

88. In addition, Plaintiff Tanzman is disabled and is currently living with disabling HIV/AIDS. Because of his weakened immune system, he has been advised by his doctor to avoid unnecessary public interactions. He thus relies on Patelco's mobile app and online banking system to manage his finances. Because those systems were offline due to the Data Breach, causing Plaintiff Tanzman to visit Patelco branches to withdraw funds, the Breach exposed him to serious risks to his health. It also caused Plaintiff Tanzman extreme stress, which may further exacerbate his condition. In one recent visit to a Patelco branch office in San Francisco following the Data Breach, Plaintiff Tanzman experienced a violent encounter, in which an unidentified man threatened to attack him with a knife. But for the Data Breach, and Plaintiff Tanzman's resulting need to visit branch offices in person, this incident would not have occurred.

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

90. Tanzman suffered actual injury in the form of damages to and diminution in the value of Tanzman's Private Information—a form of intangible property that Tanzman entrusted to Defendant, which was compromised in and as a result of the Data Breach.

91. Tanzman suffered lost time, annoyance, interference and inconvenience as a result of the Data Breach and has anxiety and increased concerns for the loss of privacy, as well as anxiety over the impact of cybercriminals accessing, using and selling Tanzman's Private Information.

92. Tanzman suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft and misuse resulting from Tanzman's Private Information being placed in the hands of unauthorized third parties and criminals.

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

93. Tanzman has a continuing interest in ensuring that his Private Information, which, upon information and belief, remains in Defendant's possession, is protected and safeguarded from future breaches.

Plaintiff Darren Van Antwerp

94. Plaintiff Darren Van Antwerp is an adult individual and, at all relevant times herein, was a resident and citizen of the State of California. Van Antwerp is a victim of the Data Breach.

95. Plaintiff Van Antwerp has been a Patelco member since 2012.

96. Defendant received highly sensitive Private Information from Van Antwerp in connection with the services Van Antwerp obtained. As a result, Van Antwerp's information was among the data accessed by an unauthorized third party in the Data Breach.

97. At all times herein relevant, Plaintiff Van Antwerp is and was a member of the Class(es).

98. Van Antwerp's Private Information was exposed in the Data Breach because Defendant stored and/or shared Van Antwerp's Private Information. Plaintiff Van Antwerp's Private Information was within the possession and control of Defendant at the time of the Data Breach.

99. As a proximate result of the Data Breach, Van Antwerp and his business and personal life have suffered from not having access to his financial accounts and online banking services.

100. When Patelco's online banking services were shutdown, Van Antwerp was forced to withdraw cash from a Patelco branch bank or an ATM to pay his daily expenses, as he lost access to his online checking and savings account. But even then, because Patelco limited customers to withdrawing only $500 a day, Van Antwerp nevertheless needed to take out loans to pay necessary expenses such as his rent, taking on debt and accruing interest he otherwise would not have accrued but for the Data Breach.

101. Furthermore, the disruption of Patelco online banking services also lead to lost financial opportunities for Van Antwerp, who runs a business of buying collectible items and reselling them. Thus, During the over-two-weeks that Patelco shutdown online banking services,

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

Van Antwerp was unable to run his business as usual as he could not purchase any collectible items to sells. Van Antwerp estimates he lost $4,000-$5,000 in terms of business opportunity.

102. Furthermore, following the Data Breach, Van Antwerp's credit score dropped significantly. Van Antwerp believes and alleges this was caused by the loans he needed to take out, which itself was proximately caused by the Data Breach.

103. Van Antwerp reports the experience of the Data Breach and the disruption of services at Patelco also caused him much stress because he is anxious about the loans he had to take out in order to pay his rent and daily expenses while Patelco's online banking services were shutdown. Van Antwerp also has concerns for his personal financial security as a result of the Data Breach given the highly personal nature of PII exposed. Van Antwerp also believes and alleges the stress may have impacted his wife who is currently six months pregnant with twins and is suffering from some medical issues often associated with stress.

104. Thus, Van Antwerp spent time dealing with the consequences of the Data Breach, which included and continues to include, time spent verifying the legitimacy and impact of the Data Breach, exploring credit monitoring and identity theft insurance options, self-monitoring his accounts and seeking legal counsel regarding his options for remedying and/or mitigating the effects of the Data Breach. This time has been lost forever and cannot be recaptured.

105. Van Antwerp suffered actual injury in the form of damages to and diminution in the value of his Private Information—a form of intangible property that Plaintiff entrusted to Defendant, which was compromised in and as a result of the Data Breach.

106. Van Antwerp suffered lost time, annoyance, interference and inconvenience as a result of the Data Breach and has anxiety and increased concerns for the loss of privacy, as well as anxiety over the impact of cybercriminals accessing, using and selling his Private Information.

107. Van Antwerp suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft and misuse resulting from his Private Information being placed in the hands of unauthorized third parties and criminals.

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

108. Van Antwerp has a continuing interest in ensuring that his Private Information, which, upon information and belief, remains in Defendant's possession, is protected and safeguarded from future breaches.

Plaintiff Darrel Adams

109. Plaintiff Darrel Adams is an adult individual and, at all relevant times herein, was a resident and citizen of the State of California. Adams is a victim of the Data Breach.

110. Defendant received highly sensitive Private Information from Adams in connection with the services Adams obtained. As a result, Adam's information was among the data accessed by an unauthorized third party in the Data Breach.

111. At all times herein relevant, Adams is and was a member of the Class(es).

112. Adams's Private Information was within the possession and control of Defendant at the time of the Data Breach.

113. Adams's Private Information was exposed in the Data Breach because Defendant stored and/or shared Adams's Private Information. Indeed, Adams received a notice from his Experian credit monitoring service notifying him that his Private Information was found on the Dark Web as a result of the Data Breach.

114. In response to the notice he received from his Experian credit monitoring service, Adams was forced to incur out-of-pocket damages in the form of him being forced to pay approximately $30-$50 to mail documents to Experian notifying them that his credit had been compromised as a result of the Data Breach. Moreover, Adams also suffered out-of-pocket damages in the form of travel expenses when he was forced to travel to and from his local Patelco branch on four separate occasions to report the fraud he suffered as a result of the Data Breach.

115. Although Patelco became aware of the Data Breach on June 29, 2024, Adams did not receive a personal notice of the breach from Patelco until August 20, 2024. This delay in notification was harmful in itself because it prevented Adams from mitigating his own damages in a timely manner.

116. To make matters even worse, Adams has experienced fraud as a result of the Data Breach. Specifically, Adams experienced two unauthorized credit card transactions on his Patelco

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

accounts for $450 each shortly after the Data Breach occurred and suffered an unknown third party attempting to log into his cryptocurrency account.

117. Moreover, since May 23, 2024 (the date Patelco alleges hackers first gained access to its computer systems), Adams has experienced a significant uptick in spam calls, texts and emails.

118. In addition, Adams experienced a debilitating disruption in his ability to access Patelco's financial services for over two weeks when Patelco shut down online banking services from June 29, 2024 to July 15, 2024. As a result, Adams was unable to access his online Patelco account or mobile banking app which, in turn, prevented him from logging in to his online banking accounts or making credit or debit card payments for this entire period. Adams reports this prevented him from paying his usual bills in a timely manner and, as a result, he incurred $35 in late fees and penalties for being unable to access his Patelco accounts that have not been reimbursed.

119. Thus, Adams spent approximately 20 hours dealing with the consequences of the Data Breach, which included and continues to include, time spent verifying the legitimacy and impact of the Data Breach, exploring credit monitoring and identity theft insurance options, self-monitoring his accounts, traveling to and from his local Patelco branch, and seeking legal counsel regarding his options for remedying and/or mitigating the effects of the Data Breach. This time has been lost forever and cannot be recaptured.

120. Adams believes and alleges that, in addition to the damages and expenses described herein, he has spent at least another $85 mitigating the risks caused by the Data Breach.

121. Adams suffered actual injury in the form of the out-of-pocket expenses described herein and damages to and diminution in the value of his Private Information—a form of intangible property that Adams entrusted to Defendant, which was compromised in and as a result of the Data Breach.

122. Adams suffered lost time, annoyance, interference and inconvenience as a result of the Data Breach and has anxiety and increased concerns for the loss of privacy, as well as anxiety over the impact of cybercriminals accessing, using and selling his Private Information.

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

123. Adams suffered concrete injuries arising from the fraud, identity theft and misuse resulting from his Private Information being placed in the hands of unauthorized third parties/criminals as described herein.

124. Adams has a continuing interest in ensuring that his Private Information, which, upon information and belief, remains in Defendant's possession, is protected and safeguarded from future breaches.

Plaintiff Wily Lee

125. Plaintiff Wily Lee is an adult individual and, at all relevant times herein, was a resident and citizen of the State of California. Lee is a victim of the Data Breach.

126. Defendant received highly sensitive Private Information from Lee in connection with the services Lee obtained. As a result, Lee's information was among the data accessed by an unauthorized third party in the Data Breach.

127. At all times herein relevant, Lee is and was a member of the Class(es).

128. Lee's Private Information was within the possession and control of Defendant at the time of the Data Breach.

129. Lee's Private Information was exposed in the Data Breach because Defendant stored and/or shared Lee's Private Information.

130. Although Patelco became aware of the Data Breach on June 29, 2024, Lee did not receive a personal notice of the breach from Patelco until August 20, 2024. This delay in notification was harmful in itself because it prevented Adams from mitigating his own damages in a timely manner.

131. Since May 23, 2024 (the date Patelco alleges hackers first gained access to its computer systems), Adams has experienced a significant uptick in spam calls, texts and emails.

132. In addition, Lee experienced a debilitating disruption in his ability to access Patelco's financial services for many days when Patelco shut down online banking services from June 29, 2024 to July 15, 2024. As a result, Lee was unable to access his online Patelco account or mobile banking app which, in turn, prevented him from logging in to his online banking

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

accounts or making credit or debit card payments for this entire period. Lee reports this forced him to borrow money from his friend in order to pay bills on time.

133. Thus, Lee spent approximately seven hours dealing with the consequences of the Data Breach, which included and continues to include, time spent verifying the legitimacy and impact of the Data Breach, exploring credit monitoring and identity theft insurance options, self-monitoring his accounts, traveling to and from his local Patelco branch, and seeking legal counsel regarding his options for remedying and/or mitigating the effects of the Data Breach. This time has been lost forever and cannot be recaptured.

134. Lee suffered actual injury in the form of the out-of-pocket expenses described herein and damages to and diminution in the value of his Private Information—a form of intangible property that Lee entrusted to Defendant, which was compromised in and as a result of the Data Breach.

135. Lee suffered lost time, annoyance, interference and inconvenience as a result of the Data Breach and has anxiety and increased concerns for the loss of privacy, as well as anxiety over the impact of cybercriminals accessing, using and selling his Private Information.

136. Lee suffered concrete injuries arising from the fraud, identity theft, and misuse resulting from his Private Information being placed in the hands of unauthorized third parties/criminals as described herein.

137. Lee has a continuing interest in ensuring that his Private Information, which, upon information and belief, remains in Defendant's possession, is protected and safeguarded from future breaches.

Plaintiff Siobhan Gallagher

138. Plaintiff Siobhan Gallagher is an adult individual and, at all relevant times herein, was a resident and citizen of the State of North Carolina. Gallagher is a victim of the Data Breach.

139. Defendant received highly sensitive Private Information from Gallagher in connection with the services Gallagher obtained. As a result, Gallagher's information was among the data accessed by an unauthorized third party in the Data Breach.

140. At all times herein relevant, Gallagher is and was a member of the Class(es).

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

141. Gallagher's Private Information was within the possession and control of Defendant at the time of the Data Breach.

142. Gallagher's Private Information was exposed in the Data Breach because Defendant stored and/or shared Gallagher's Private Information. Indeed, Gallagher received a fraud alert email from Chase Bank notifying her of potential fraud which is a clear indication of fraudulent activity using her Private Information because she does not have an account with Chase Bank.

143. Moreover, Gallagher also suffered out-of-pocket damages in the form of approximately $30.45 in postage and when he was forced to send a complaint to the National Credit Union Complaint Agency as a result of the Data Breach and resulting service disruption and travel expenses as a result of her being forced to travel to and from her local Patelco branch as a result of the Data Breach.

144. Although Patelco became aware of the Data Breach on June 29, 2024, Gallagher did not receive a personal notice of the breach from Patelco until August 20, 2024. This delay in notification was harmful in itself because it prevented Gallagher from mitigating her own damages in a timely manner.

145. Moreover, since May 23, 2024 (the date Patelco allages hackers first gained access to its computer systems), Gallagher has experienced a significant uptick in spam calls, texts and emails.

146. In addition, Gallagher experienced a debilitating disruption in her ability to access Patelco's financial services for over two weeks when Patelco shut down online banking services from June 29, 2024 to July 15, 2024. As a result, Gallagher was unable to access her online Patelco account or mobile banking app which, in turn, prevented her from logging in to his online banking accounts or making credit or debit card payments for this entire period. Gallagher reports this prevented her from paying her usual bills in a timely manner and, as a result, she incurred service fees due to her account being overdrawn. This resulted in Gallagher being forced to write a complaint to the National Credit Union Complaint Agency explaining the situation and move funds from her retirement accounts to her Patelco accounts to cover the overdraft charges.

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

147. Shockingly, Gallagher still does not have access to her money with Patelco, is unable to withdraw any money from her account, and is unable to use her Master Card or debit card only further exacerbating the harms she has suffered as a result of the Data Breach and resulting service interruptions.

148. Thus, Gallagher spent approximately 40 hours dealing with the consequences of the Data Breach, which included and continues to include, time spent verifying the legitimacy and impact of the Data Breach, exploring credit monitoring and identity theft insurance options, self-monitoring her accounts, traveling to and from her local Patelco branch, writing complaints, speaking to Patelco representatives, and seeking legal counsel regarding her options for remedying and/or mitigating the effects of the Data Breach. This time has been lost forever and cannot be recaptured.

149. Gallagher suffered actual injury in the form of the out-of-pocket expenses described herein and damages to and diminution in the value of her Private Information—a form of intangible property that Gallagher entrusted to Defendant, which was compromised in and as a result of the Data Breach.

150. Gallagher suffered lost time, annoyance, interference and inconvenience as a result of the Data Breach and has anxiety and increased concerns for the loss of privacy, as well as anxiety over the impact of cybercriminals accessing, using and selling her Private Information.

151. Gallagher suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft and misuse resulting from his Private Information being placed in the hands of unauthorized third parties/criminals.

152. Gallagher has a continuing interest in ensuring that her Private Information, which, upon information and belief, remains in Defendant's possession, is protected and safeguarded from future breaches.

Plaintiff Sean McGinity

153. Plaintiff Sean McGinity is an adult individual and, at all relevant times herein, was a resident and citizen of the State of California. McGinity is a victim of the Data Breach.

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

154. Defendant received highly sensitive Private Information from McGinity in connection with the services he obtained. As a result, McGinity's Private Information was within the possession and control of Defendant at the time of the Data Breach and was among the data accessed by an unauthorized third party in the Data Breach.

155. At all times herein relevant, McGinity is and was a member of the Class(es).

156. McGinity's Private Information was exposed in the Data Breach because Defendant stored and/or shared his Private Information.

157. Since May 23, 2024 (the date Patelco alleges hackers first gained access to its computer systems), McGinity has experienced a significant uptick in spam calls, texts and emails.

158. In addition, McGinity experienced a debilitating disruption in his ability to access Patelco's financial services for many days when Patelco shut down online banking services from June 29, 2024 to July 15, 2024. As a result, McGinity was unable to access his online Patelco account or mobile banking app which, in turn, prevented him from logging in to his online banking accounts or making credit or debit card payments for this entire period. Because of the disruption, a previous loan held by McGinity was not paid off, and he incurred and paid additional interest he would not have otherwise paid as a result.

159. Thus, McGinity spent approximately five hours dealing with the consequences of the Data Breach, which included and continues to include time spent verifying the legitimacy and impact of the Data Breach, exploring credit monitoring and identity theft insurance options, self-monitoring his accounts, traveling to and from his local Patelco branch and seeking legal counsel regarding his options for remedying and/or mitigating the effects of the Data Breach. This time has been lost forever and cannot be recaptured.

160. McGinity suffered actual injury in the form of the out-of-pocket expenses described herein and damages to and diminution in the value of his Private Information—a form of intangible property that McGinity entrusted to Defendant, which was compromised in and as a result of the Data Breach.

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

161. McGinity suffered lost time, annoyance, interference and inconvenience as a result of the Data Breach and has anxiety and increased concerns for the loss of privacy, as well as anxiety over the impact of cybercriminals accessing, using and/or selling his Private Information.

162. McGinity suffered concrete injuries arising from the fraud, identity theft, and misuse resulting from his Private Information being placed in the hands of unauthorized third parties/criminals as described herein.

163. McGinity has a continuing interest in ensuring that his Private Information, which, upon information and belief, remains in Defendant's possession, is protected and safeguarded from future breaches.

Plaintiff Daniel Corona

164. Plaintiff Daniel Corona is an adult individual and, at all relevant times herein, was a resident and citizen of the State of California. Corona is a victim of the Data Breach.

165. Defendant received highly sensitive Private Information from Corona in connection with the services he obtained. As a result, Corona's Private Information was within the possession and control of Defendant at the time of the Data Breach and was among the data accessed by an unauthorized third party in the Data Breach.

166. At all times herein relevant, Corona is and was a member of the Class(es).

167. Corona's Private Information was exposed in the Data Breach because Defendant stored and/or shared his Private Information.

168. Since May 23, 2024 (the date Patelco alleges hackers first gained access to its computer systems), Corona has experienced a significant uptick in spam calls, texts and emails.

169. In addition, Corona experienced a debilitating disruption in his ability to access Patelco's financial services for many days (i.e., when Patelco shut down online banking services from June 29, 2024 to July 15, 2024). As a result, Corona was unable to access his online Patelco account or mobile banking app which, in turn, prevented him from logging in to his online banking accounts or making credit or debit card payments for this entire period. Corona thus incurred late fees on personal loans he would not have otherwise incurred.

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

170. Moreover, Corona received notice from his credit monitoring service on July 23, 2024 that his PII was located on the dark web.

171. Thus, Corona spent approximately five hours dealing with the consequences of the Data Breach, which included and continues to include time spent verifying the legitimacy and impact of the Data Breach, exploring credit monitoring and identity theft insurance options, self-monitoring his accounts, traveling to and from his local Patelco branch, and seeking legal counsel regarding his options for remedying and/or mitigating the effects of the Data Breach. This time has been lost forever and cannot be recaptured.

172. Corona suffered actual injury in the form of the out-of-pocket expenses described herein and damages to and diminution in the value of his Private Information—a form of intangible property that Corona entrusted to Defendant, which was compromised in and as a result of the Data Breach.

173. Corona suffered lost time, annoyance, interference and inconvenience as a result of the Data Breach and has anxiety and increased concerns for the loss of privacy, as well as anxiety over the impact of cybercriminals accessing, using and selling his Private Information.

174. Corona suffered concrete injuries arising from the fraud, identity theft and misuse resulting from his Private Information being placed in the hands of unauthorized third parties/criminals as described herein.

175. Corona has a continuing interest in ensuring that his Private Information, which, upon information and belief, remains in Defendant's possession, is protected and safeguarded from future breaches.

DEFENDANT

176. Defendant is a corporation with a principal place of business located in Dublin, California. Defendant is the 22nd largest credit union serving Northern California, particularly serving the San Francisco Bay Area.[6] Further, Defendant advertises "$9 billion in assets and over 450,000 members nationwide[.]"[7]

[6] https://www.patelco.org/about-patelco/who-we-are/ (last accessed, July 3, 2024).

[7] Who We Are, PATELCO CREDIT UNION, https://www.patelco.org/about-patelco/who-we-are (last visited Oct. 2, 2024).

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

177. Defendant offers a wide range of financial services, including checking and savings accounts, loans, credit cards, investment services and insurance plans.

178. 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 Plaintiffs. Representative Plaintiffs will seek leave of court to amend this Complaint to reflect the true names and capacities of such responsible parties when their identities become known.

179. Defendants Does 1 through 50 are presently unknown to Plaintiffs. Pursuant to Cal. Civ. Proc. Code § 474, Plaintiffs are unaware of the true names and capacities of these Defendants and, therefore, bring suit against these Defendants under fictitious names. Plaintiffs will seek to amend this Complaint and include these Doe Defendants' true names and capacities when they are ascertained. Each of the fictitiously named Defendants is responsible in some capacity for the conduct alleged and wrongs described herein.

CLASS ACTION ALLEGATIONS

180. Representative Plaintiffs bring this action pursuant to the provisions of California Code of Civil Procedure § 382 on behalf of Representative Plaintiffs and the following classes (collectively, the "Classes"):

> **California Class:**
> All individuals residing within the State of California whose Private Information was exposed to unauthorized third parties as a result of the data breach discovered by Defendant on or before June 29, 2024.
>
> **Nationwide Class:**
> All individuals residing within the United States of America whose Private Information was exposed to unauthorized third parties as a result of the data breach discovered by Defendant on or before June 29, 2024.

181. 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,

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

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

182. Pursuant to California Rule of Court, Rule 3.765(b), Representative Plaintiffs reserve the right to amend or modify the class definition to achieve greater specificity by further division into sub-classes and/or by limitation to particular issues.

183. This action has been brought and may properly be maintained as a class action under California Code of Civil Procedure § 382 because there is a well-defined community of interest in the litigation and membership in the proposed Classes are 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 Classes will be determined by analysis of Defendant's records.

b. Commonality: Representative Plaintiffs 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 Plaintiffs 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;

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

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 Plaintiffs 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 Plaintiffs' and Class Members' Private Information;

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 Representative Plaintiffs' and Class Members' Private Information;

11) Whether Representative Plaintiffs 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 Plaintiffs and Class Members are entitled to restitution as a result of Defendant's wrongful conduct.

c. Typicality: Representative Plaintiffs' claims are typical of the claims of the Plaintiff Classes. Representative Plaintiffs 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 Plaintiffs in this class action is an adequate representative of each of the Plaintiff Classes in that the

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

Representative Plaintiffs have 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 entireties. Representative Plaintiffs 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.

184. Class certification is proper because the questions raised by this Complaint are of common or general interest affecting so many individuals that it is impracticable to bring all Class Members before the Court.

185. 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 Class(es) in their entireties. Defendant's policies and practices challenged herein apply to and affect Class Members uniformly and Representative Plaintiffs' challenge of these policies and practices hinges on Defendant's

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

conduct with respect to the Classes in their entireties, not on facts or law applicable only to Representative Plaintiffs.

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

187. Further, Defendant has acted or refused to act on grounds generally applicable to the Classes and, accordingly, final injunctive or corresponding declaratory relief with regard to the Class Members as a whole is appropriate under California Code of Civil Procedure § 382.

COMMON FACTUAL ALLEGATIONS

The Cyberattack

188. In the course of the Data Breach, one or more unauthorized third parties accessed Class Members' Private Information. Representative Plaintiffs were among the individuals whose data was accessed in the Data Breach.

189. According to the Data Breach Notification and/or publicly filed documents, Representative Plaintiffs state, on information and belief, that millions of persons were affected by the Data Breach.

190. On June 29, 2024, Patelco experienced a ransomware attack, in which cybercriminals used malware to infiltrate its computer systems and encrypted them, then demanded a ransom to unlock them.

191. At the time, Defendant stated, "Unfortunately, this incident has required us to proactively shut down some of our day-to-day banking systems in order to contain and remediate the issue."[8]

192. As a result, Patelco shut down online banking for its members, rendering them unable to access their accounts for basic activity like viewing their balances, making electronic transfers. and scheduling new online bill payments. Services including online banking, mobile apps, monthly statements, Zelle transactions, balance inquiries, new or edited bill payments and

[8] Security Incident Updates & Information Center, PATELCO CREDIT UNION, https://www.patelco.org/about-patelco/who-we-are (last visited Oct. 2, 2024).

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

check cashing were offline and unavailable.[9] The shutdown of these critical online banking services lasted for over two weeks, finally being restored on July 15, 2024.[10]

193. Furthermore, the shutdown caused Plaintiffs and Class Members enormous harm, including bounced payments and late-payment and overdraft fees. The inability of Plaintiffs and Class Members to access their online banking systems left them unable to manage their financial lives and, as a result, these outages may negatively affect their credit scores.

194. As of the writing of this complaint, Patelco has provided little information about who was responsible for the attack, how much was demanded as ransom, whether it paid the ransom, and how many people were affected by the cyberattack. A Patelco spokesperson told the San Francisco Chronicle that she was unable to provide further information about the incident, saying only that Patelco was "committed to supporting our members."[11]

195. On August 16, 2024 Patelco was added to the website belonging to a ransomware group going by the name of "RansomHub," who claimed responsibility for the ransomware attack in a post on its website.[12] In the post, the cybercriminals claimed they conducted negotiations with Patelco for two weeks but could not reach an agreement and, consequently, the hackers purported to offer the stolen PII for sale in an auction on their website.[13] Additionally, although Patelco's website says it has over 450,000 members, according to the Maine Attorney General's Office, the Data Breach has actually impacted approximately 1,009,472 current and former customers and employees of Patelco.[14]

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

---

[9] *Id.*

[10] Annie Sciacca, *2 weeks after ransomware attack, Patelco restores most banking functions*, THE OAKLANDSIDE, (July 15, 2024), https://oaklandside.org/2024/07/15/ransomware-patelco-credit-union-restores-most-banking-functions-2/.

[11] Jessica Flores, *Massive Patelco cyberattack is still affecting half a million people. Here's how to protect yourself*, SAN FRANCISCO CHRONICLE (July 12, 2024), https://www.sfchronicle.com/bayarea/article/patelco-lawsuits-struggling-to-recover-cyberattack-19569709.php.

[12] Eduard Kovacs, *Patelco Credit Union Says Breach Impacts 726K After Ransomware Gang Auctions Data,* SECURITY WEEK (August 26, 2024), https://www.securityweek.com/patelco-credit-union-says-breach-impacts-726k-after-ransomware-gang-auctions-data/.

[13] *Id.*

[14] *See, supra,* n.1.

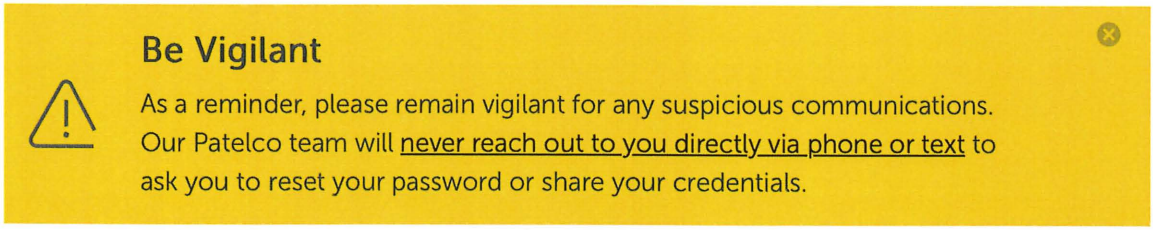
196. On July 3, 2024, Patelco stated that its "cyber security specialists have validated and greenlighted [its] core systems – your money is safe and secure."[15]

197. On July 13, 2024, Patelco CEO Erin Mendez wrote that "we have meticulously examined and bolstered our environment in order to bring our systems back online. Cybersecurity defense is a constantly moving target, particularly for financial services institutions, which are often targets for these kinds of attacks. We remain committed to making strategic investments in the advanced tools, teams, and partners that help keep us safe."[16]

198. Although Patelco has failed to provide any detail about these "strategic investments" to bolster the company's cybersecurity, such policies and practices clearly should have been in place and fully operational *before* the Data Breach.

199. As a result—and despite Patelco's repeated commitments and assurances to its customers—Plaintiffs' and Class Members' highly sensitive PII was leaked and offered for sale on the Dark Web by cybercriminals.

200. Through its public communications, Patelco has also recognized the actual imminent harm and injury that flowed from the Data Breach. In a bright yellow banner at the top of every page of its website, it warns its members to "Be Vigilant," reminding its members to "please remain vigilant for any suspicious communications."[17]



201. Indeed, the Data Breach involves PII that is difficult or even impossible to change, such as Social Security numbers and dates of birth. Further, the Data Breach exposed nonpublic, highly private information, which is disturbing harm in and of itself. Even with complimentary short-term identity monitoring services, the risk of identity theft and unauthorized use of Plaintiffs'

[15] *Id.*
[16] *Id.*
[17] *Id.*

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

and Class Members' PII remains very high. Some of the fraudulent activity resulting from the Data Breach may not come to light for years.

Defendant's Failed Response to the Breach

202. Upon information and belief, the unauthorized third-party cybercriminals gained access to Representative Plaintiffs' and Class Members' Private Information with the intent of misusing the Private Information, including marketing and selling Representative Plaintiffs' and Class Members' Private Information.

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

204. Despite first becoming aware of the Data Breach on June 29, 2024, Patelco did not provide personal notice of the Data Breach to Plaintiffs until on or about August 20, more than seven weeks later. Specifically, the notice emailed to Plaintiffs acknowledged that an "investigation revealed that an unauthorized party gained access to [Patelco's] network on May 23, 2024, leading to access to the database on June 29, 2024."[18] But despite finally disclosing the Data Breach to Plaintiffs and acknowledging in the notice that "the accessed databases contained your personal information," Patelco has failed to provide more specific details about the personal information that was accessed, simply stating that "the specific data that was accessed has not been determined."[19]

205. In the same notice Patelco also acknowledged that at the least the PII contained in the accessed database "included first and last name with Social Security number, Driver's license

[18] *See, supra,* n.6.

[19] *Id.*

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

number, date of birth, and/or email address," but "[n]ot every data element was present for every individual."[20]

206. Such a notice written in vague terms is too little, too late. As noted above, Patelco still has not provided any explanation or justification for its more than seven-week delay in notifying the Plaintiffs and Class Members that their PII had been accessed in the Data Breach. This delay in notification caused Plaintiffs substantial harm independent of the harm caused by the Data Breach itself because it prevented Plaintiffs from taking timely preventative measures to mitigate their own damages.

207. Furthermore, although in its notice letter Patelco offered Plaintiffs a two-year membership to Experian, an identity-protection service, such an offer is insufficient considering the fact that once an individual's PII has been leaked online or posted to the Dark Web, that individual will likely have to contend with instances of identity theft or fraud for the rest of their life. As such, Patelco's notice to Plaintiffs was both untimely and provided insufficient remedies to Plaintiffs and Class Members.

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

Defendant Collected/Stored Class Members' Private Information

209. Defendant acquired, collected, stored and assured reasonable security over Representative Plaintiffs' and Class Members' Private Information.

210. As a condition of its relationships with Representative Plaintiffs and Class Members, Defendant required that each Representative Plaintiff and Class Member entrust Defendant with highly sensitive and confidential Private Information. Defendant, in turn, stored that information on Defendant's system that was ultimately affected by the Data Breach.

[20] *Id.*

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

211. Under state and federal law, businesses like Defendant have duties to protect its current and former customers' PII and to notify them about breaches.

212. Defendant recognizes these duties, declaring in its "Privacy Policy"[21] that:

a. "Your privacy is very important to us."

b. "At Patelco, we respect your right to privacy and understand the importance of maintaining the security of your personal information."

c. "This is another way we are looking out for your financial wellbeing."

d. The security of your personal and financial information is our highest priority."

213. Likewise, in its "Federal Privacy Notice,"[22] Defendant provides that that:

a. "Financial companies choose how they share your personal information."

b. "To protect your personal information from unauthorized access and use, we use security measures that comply with federal law."

c. "These measures include computer safeguards and secured files and buildings. Credit Union staff, management and volunteers are trained to keep consumer information strictly confidential."

214. By obtaining, collecting and storing Representative Plaintiffs' and Class Members' Private Information, Defendant assumed legal and equitable duties over the Private Information and knew or should have known that it was thereafter responsible for protecting Representative Plaintiffs' and Class Members' Private Information from unauthorized disclosure.

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

---

[21] Privacy Policy, PATELCO CREDIT UNION (March 20, 2023), https://www.patelco.org/privacy.

[22] Federal Privacy Notice, PATELCO CREDIT UNION (March 20, 2023), https://www.patelco.org/wp-content/uploads/2023/05/Federal-Privacy-Notice.pdf.

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

216. Defendant could have prevented the Data Breach by properly securing and encrypting and/or more securely encrypting its servers generally, as well as Representative Plaintiffs' and Class Members' Private Information.

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

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

219. And yet, despite the prevalence of public announcements of data breach and data security compromises, Defendant failed to take appropriate steps to protect Representative Plaintiffs' and Class Members' Private Information from being compromised.

Defendant Had an Obligation to Protect the Stolen Information

220. In failing to adequately secure Representative Plaintiffs' and Class Member's sensitive data, Defendant breached duties it owed Representative Plaintiffs and Class Members under statutory and common law.

221. Representative Plaintiffs and Class Members surrendered their highly sensitive Private Information to Defendant under the implied condition that Defendant would keep it private and secure. Accordingly, Defendant also has an implied duty to safeguard their Private Information, independent of any statute. Defendant was also prohibited by the Federal Trade Commission Act (the "FTC Act") (15 U.S.C. § 45) from engaging in "unfair or deceptive acts or practices in or affecting commerce." The Federal Trade Commission (the "FTC") has concluded that a company's failure to maintain reasonable and appropriate data security for consumers' sensitive personal information is an "unfair practice" in violation of the FTC Act. *See, e.g., FTC v. Wyndham Worldwide Corp.*, 799 F.3d 236 (3d Cir. 2015).

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

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

224. Defendant owed a duty to Representative Plaintiffs and Class Members to create and implement reasonable data security practices and procedures to protect all Private Information in its possession, including not sharing information with other entities who maintained sub-standard data security systems.

225. Defendant owed a duty to Representative Plaintiffs and Class Members to implement processes that would immediately detect a breach of its data security systems in a timely manner.

226. Defendant owed a duty to Representative Plaintiffs and Class Members to act upon data security warnings and alerts in a timely fashion.

227. Defendant owed a duty to Representative Plaintiffs and Class Members to disclose if its computer systems and data security practices were inadequate to safeguard individuals' Private Information from theft because such an inadequacy would be a material fact in the decision to entrust their Private Information to Defendant.

228. Defendant owed a duty of care to Representative Plaintiffs and Class Members because they were foreseeable and probable victims of any inadequate data security practices.

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

229. Defendant owed a duty to Representative Plaintiffs and Class Members to encrypt and/or more reliably encrypt Representative Plaintiffs' and Class Members' Private Information and monitor user behavior and activity in order to identity possible threats.

Value of the Sensitive Information

230. Private Information is a valuable commodity for which a "cyber black market" exists in which criminals openly post stolen payment card numbers, Social Security numbers and other personal information on a number of underground internet websites.

231. The high value of Private Information to criminals is further evidenced by the prices they will pay for it through the dark web. Numerous sources cite dark web pricing for stolen identity credentials. For example, personal information can be sold at a price ranging from $40 to $200, and bank details have a price range of $50 to $200.[23] Experian reports that a stolen credit or debit card number can sell for $5 to $110 on the dark web.[24] Criminals can also purchase access to entire company data breaches from $999 to $4,995.[25]

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

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

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

[23] *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] *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] *In the Dark*, VPNOverview, 2019, *available at*: https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/.

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

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

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

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

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

237. The harm to Representative Plaintiffs and Class Members is especially acute given the nature of the leaked data.

---

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

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

238. When cybercriminals access financial information, health insurance information and other personally sensitive data—as they did here—there is no limit to the amount of fraud to which Defendant may have exposed Representative Plaintiffs and Class Members. The exposure of any Private Information can cause unexpected harms one would not ordinarily associate with the type of information stolen. Cybercriminals routinely aggregate Private Information from multiple illicit sources and use stolen information to gather even more information through social engineering, credential stuffing and other methods. The resulting complete dossiers of Private Information are particularly prized among cybercriminals because they expose the target to every manner of identity theft and fraud.

239. Identity thieves can use Private Information such as that exposed in the Data Breach to: (a) apply for credit cards or loans (b) purchase prescription drugs or other medical services (c) commit immigration fraud; (d) obtain a fraudulent driver's license or ID card in the victim's name; (e) obtain fraudulent government benefits or insurance benefits; (f) file a fraudulent tax return using the victim's information; (g) commit espionage; or (h) commit any number of other frauds, such as obtaining a job, procuring housing, or giving false information to police during an arrest.

240. Annual monetary losses for victims of identity theft are in the billions of dollars. In 2017, fraudsters stole $16.8 billion from consumers in the United States, which includes $5.1 billion stolen through bank account take-overs.[56]

241. The annual cost of identity theft is even higher. McAfee and the Center for Strategic and International Studies estimates that the likely annual cost to the global economy from cybercrime is $445 billion a year.[57]

242. Reimbursing a consumer for a financial loss due to fraud does not make that individual whole again. On the contrary, in addition to the irreparable damage that may result from the theft of a Social Security number, identity theft victims must spend numerous hours and their own money repairing the impact to their credit. After conducting a study, the Department of Justice's Bureau of Justice Statistics found that identity theft victims "reported spending an average of about 7 hours clearing up the issues" and resolving the consequences of fraud in 2014.

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

243. And, the impact of identity theft can have ripple effects, which can adversely affect the future financial trajectories of victims' lives. For example, the Identity Theft Resource Center reports that respondents to their surveys in 2013-2016 described that the identity theft they experienced affected their ability to get credit cards and obtain loans such as student loans or mortgages. For some victims, this could mean the difference between going to college or not, becoming a homeowner or not, or having to take out a high interest payday loan versus a lower-interest loan. It is no wonder then that identity theft exacts a severe emotional toll on its victims.

244. And data breaches are preventable.[27] As Lucy Thompson wrote in the DATA BREACH AND ENCRYPTION HANDBOOK, "[i]n almost all cases, the data breaches that occurred could have been prevented by proper planning and the correct design and implementation of appropriate security solutions."[28] She added that "[o]rganizations that collect, use, store, and share sensitive personal data must accept responsibility for protecting the information and ensuring that it is not compromised...."[29]

245. Most of the reported data breaches are a result of lax security and the failure to create or enforce appropriate security policies, rules and procedures. Appropriate information security controls, including encryption, must be implemented and enforced in a rigorous and disciplined manner so that a *data breach never occurs*.[30]

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

---

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

[28] *Id.* at 17.

[29] *Id.* at 28.

[30] *Id.*

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

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

FIRST CAUSE OF ACTION
Negligence

248. 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 herein.

249. At all times herein relevant, Defendant owed Representative Plaintiffs and Class Members a duty of care, *inter alia*, to act with reasonable care to secure and safeguard their Private Information and to use commercially reasonable methods to do so. Defendant took on this obligation upon accepting and storing Representative Plaintiffs' and Class Members' Private Information on its computer systems and networks.

250. Among these duties, Defendant was expected:

a. to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting and protecting the Private Information in its possession;

b. to protect Representative Plaintiffs' and Class Members' Private Information using reasonable and adequate security procedures and systems that were/are compliant with industry-standard practices;

c. to implement processes to quickly detect the Data Breach and to timely act on warnings about data breaches; and

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

d. to promptly notify Representative Plaintiffs and Class Members of any data breach, security incident or intrusion that affected or may have affected their Private Information.

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

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

253. Defendant knew or should have known that its data systems and networks did not adequately safeguard Representative Plaintiffs' and Class Members' Private Information.

254. Only Defendant was in the position to ensure that its systems and protocols were sufficient to protect the Private Information that Representative Plaintiffs and Class Members had entrusted to it.

255. Defendant breached its duties to Representative Plaintiffs and Class Members by failing to provide fair, reasonable or adequate computer systems and data security practices to safeguard Representative Plaintiffs' and Class Members' Private Information.

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

257. Representative Plaintiffs' and Class Members' willingness to entrust Defendant with its Private Information was predicated on the understanding that Defendant would take adequate security precautions. Moreover, only Defendant had the ability to protect its systems and the Private Information is stored on them from attack. Thus, Defendant had a special relationship with Representative Plaintiffs and Class Members.

258. Defendant also had independent duties under state and federal laws that required Defendant to reasonably safeguard Representative Plaintiffs' and Class Members' Private

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

Information and promptly notify them about the Data Breach. These "independent duties" are untethered to any contract between Defendant and Representative Plaintiffs and/or the remaining Class Members.

259. Defendant breached its general duty of care to Representative Plaintiffs and Class Members in, but not necessarily limited to, the following ways:

a. by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Representative Plaintiffs' and Class Members' Private Information;

b. by failing to timely and accurately disclose that Representative Plaintiffs' and Class Members' Private Information had been improperly acquired or accessed;

c. by failing to adequately protect and safeguard the Private Information by knowingly disregarding standard information security principles, despite obvious risks, and by allowing unmonitored and unrestricted access to unsecured Private Information;

d. by failing to provide adequate supervision and oversight of the Private Information with which it was and is entrusted, in spite of the known risk and foreseeable likelihood of breach and misuse, which permitted an unknown third party to gather Representative Plaintiffs' and Class Members' Private Information, misuse the Private Information and intentionally disclose it to others without consent;

e. by failing to adequately train its employees to not store Private Information longer than absolutely necessary;

f. by failing to consistently enforce security policies aimed at protecting Representative Plaintiffs' and the Class Members' Private Information;

g. by failing to implement processes to quickly detect data breaches, security incidents or intrusions; and

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

h. by failing to encrypt Representative Plaintiffs' and Class Members' Private Information and monitor user behavior and activity in order to identify possible threats.

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

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

262. The law further imposes an affirmative duty on Defendant to timely disclose the unauthorized access and theft of the Private Information to Representative Plaintiffs 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 their Private Information.

263. Defendant breached its duty to notify Representative Plaintiffs and Class Members of the unauthorized access by waiting for two months after learning of the Data Breach to notify Representative Plaintiffs and Class Members and then by failing and continuing to fail to provide Representative Plaintiffs and Class Members sufficient information regarding the breach. To date, Defendant has not provided sufficient information to Representative Plaintiffs and Class Members regarding the extent of the unauthorized access and continues to breach its disclosure obligations to Representative Plaintiff and Class Members.

264. Further, through its failure to provide timely and clear notification of the Data Breach to Representative Plaintiff and Class Members, Defendant prevented Representative Plaintiffs and Class Members from taking meaningful, proactive steps to, *inter alia*, secure and/or access their Private Information.

265. There is a close causal connection between Defendant's failure to implement security measures to protect Representative Plaintiffs' and Class Members' Private Information and the harm suffered, or risk of imminent harm suffered, by Representative Plaintiffs and Class Members. Representative Plaintiffs' 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

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

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

267. The damages Representative Plaintiffs and Class Members have suffered (as alleged above) and will continue to suffer were and are the direct and proximate result of Defendant's grossly negligent conduct.

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

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

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

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

subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect Representative Plaintiffs' and Class Members' Private Information in its continued possession and (viii) future costs in terms of time, effort and money that will be expended to prevent, detect, contest and repair the impact of the Private Information compromised as a result of the Data Breach for the remainder of the lives of Representative Plaintiffs and Class Members.

271. As a direct and proximate result of Defendant's negligence and negligence *per se*, Representative Plaintiffs and Class Members have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy and other economic and noneconomic losses.

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

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

SECOND CAUSE OF ACTION
Breach of Implied Contract

273. 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 herein.

274. Through their course of conduct, Defendant, Representative Plaintiffs and Class Members entered into implied contracts for Defendant to implement data security adequate to safeguard and protect the privacy of Representative Plaintiffs' and Class Members' Private Information.

275. Defendant solicited, invited and required Representative Plaintiffs and Class Members to provide their Private Information as part of Defendant's regular business practices. Representative Plaintiffs and Class Members accepted Defendant's offers and provided their Private Information to Defendant.

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

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

278. Representative Plaintiffs and Class Members fully performed their obligations under the implied contracts with Defendant.

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

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

THIRD CAUSE OF ACTION
Breach of the Implied Covenant of Good Faith and Fair Dealing

281. 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.

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

282. 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.

283. Representative Plaintiffs and Class Members have complied with and performed all conditions of their contracts with Defendant.

284. Defendant breached the implied covenant of good faith and fair dealing by failing to maintain adequate computer systems and data security practices to safeguard Private Information, failing to timely and accurately disclose the Data Breach to Representative Plaintiffs and Class Members and continued acceptance of Private 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.

285. Defendant acted in bad faith and/or with malicious motive in denying Representative Plaintiffs 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.

FOURTH CAUSE OF ACTION
Violation of the California Unfair Competition Law
Cal. Bus. & Prof. Code §§ 17200, *et seq.*
(On Behalf of Plaintiffs and the California Subclass)

286. 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 herein

287. Defendant is a "person" as defined by Cal. Bus. & Prof. Code §17201.

288. Defendant violated Cal. Bus. & Prof. Code § 17200, *et seq.* ("UCL") by engaging in unlawful, unfair and deceptive business acts and practices.

289. Defendant's "unfair" acts and practices include:

a. Defendant's failure to implement and maintain reasonable security measures to protect Representative Plaintiffs' and Class Members' Private Information from unauthorized disclosure, release, data breaches and theft, which was a direct and proximate cause of the Data Breach. Defendant failed to identify foreseeable security risks, remediate identified security

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

risks and adequately maintain and/or improve security following previous cybersecurity incidents. This conduct, with little if any utility, is unfair when weighed against the harm to Representative Plaintiffs and Class Members, whose Private Information has been compromised;

b. Defendant's failure to implement and maintain reasonable security measures, which was contrary to legislatively declared public policy that seeks to protect consumers' data and ensure that entities that are trusted with it use appropriate security measures. These policies are reflected in laws, including the FTC Act (15 U.S.C. § 45, *et seq.*);

c. Defendant's failure to implement and maintain reasonable security measures, which also leads to substantial consumer injuries, as described above, that are not outweighed by any countervailing benefits to consumers or competition. Moreover, because consumers could not know of Defendant's inadequate security, consumers could not have reasonably avoided the harms that Defendant caused;

d. Engaging in unlawful business practices by violating Cal. Civ. Code § 1798.82.

290. Defendant has engaged in "unlawful" business practices by violating multiple laws, including California's Consumer Records Act, Cal. Civ. Code §§ 1798.81.5. (requiring reasonable data security measures) and 1798.82 (requiring timely breach notification), California's Consumers Legal Remedies Act, Cal. Civ. Code § 1780, *et seq.*, the FTC Act, 15 U.S.C. § 45, *et seq.* and California common law.

291. Defendant's unlawful, unfair and deceptive acts and practices include:

a. Failing to implement and maintain reasonable security and privacy measures to protect Representative Plaintiffs' and Class Members' Private Information, which was a direct and proximate cause of the Data Breach;

b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks and adequately maintain and/or

improve security and privacy measures, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Representative Plaintiffs' and Class Members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, *et seq.,* which was a direct and proximate cause of the Data Breach;

d. Misrepresenting that it would protect the privacy and confidentiality of Representative Plaintiffs' and Class Members' Private Information, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Representative Plaintiffs' and Class Members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, *et seq.;*

f. Omitting, suppressing and concealing the material fact that it did not reasonably or adequately secure Representative Plaintiffs' and Class Members' Private Information; and

g. Omitting, suppressing and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Representative Plaintiffs' and Class Members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, *et seq.*

292. Defendant's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Defendant's data security and ability to protect the confidentiality of consumers' Private Information.

293. As a direct and proximate result of Defendant's unfair, unlawful and fraudulent acts and practices, Representative Plaintiffs and Class Members were injured and lost money or property, including the price received by Defendant for its goods and services, monetary damages from fraud and identity theft, time and expenses related to monitoring their financial accounts for

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

fraudulent activity, an increased, imminent risk of fraud and identity theft and loss of value of their Private Information.

294. Defendant acted intentionally, knowingly and maliciously to violate California's Unfair Competition Law and recklessly disregarded Representative Plaintiffs' and Class Members' rights.

295. Representative Plaintiffs and Class Members seek all monetary and nonmonetary relief allowed by law, including restitution of all profits stemming from Defendant's unfair, unlawful and fraudulent business practices or use of their Private Information, declaratory relief, reasonable attorneys' fees and costs under California Code of Civil Procedure § 1021.5, injunctive relief and other appropriate equitable relief.

FIFTH CAUSE OF ACTION
Violation of the California Consumer Privacy Act of 2018
Cal. Civ. Code §§ 1798.100, *et seq.*
(On Behalf of Plaintiffs and the California Subclass)

296. Representative Plaintiffs, individually and on behalf of the Subclass, incorporate by reference each of the factual allegations contained in the preceding paragraphs as if fully set forth herein.

297. The California Consumer Privacy Act of 2018, Cal. Civ. Code §§ 1798.100, *et seq.* ("CCPA"), was enacted to protect individuals' PII from collection and use by businesses without appropriate notice and consent.

298. Through the conduct and actions complained of herein, Defendant violated the CCPA by subjecting Representative Plaintiffs and California Subclass Members' nonencrypted PII to unauthorized access and exfiltration, theft, or disclosure as a result of Defendant's violation of its duties to implement and maintain reasonable security procedures and practices appropriate to the nature and protection of that information. Defendant thereby violated Cal. Civ. Code § 1798.150(a).

299. As a direct and proximate result of Defendant's acts, Representative Plaintiffs and the California Subclass's unencrypted and unredacted PII was subjected to unauthorized access and exfiltration, theft, or disclosure through Defendant's computer networks, servers and systems.

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

300. As a direct and proximate result of Defendant's acts, Representative Plaintiffs and the California Subclass were injured and lost money or property, including but not limited to the loss of the California Subclass's legally protected interest in the confidentiality and privacy of their PII, nominal damages and additional losses as described above.

301. Defendant knew or should have known that its computer systems, servers and networks and data security practices were inadequate to safeguard the California Subclass's PII and that the risk of a serious data breach or theft was highly likely. Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information of Plaintiffs and the California Subclass.

302. Representative Plaintiffs and the California Subclass Members are "consumers" within the meaning of Cal. Civ. Code § 1798.140(i) because they are California residents.

303. Defendant collected Representative Plaintiffs and the California Subclass's "personal information" within the meaning of Cal. Civ. Code §§ 1798.140(v) and 1798.80(e).

304. Defendant is a corporation organized or operated for the profit or financial benefit of its shareholders or other owners. Defendant "collected" Representative Plaintiffs and the California Subclass's "personal information" within the meaning of P § 1798.140(v). Defendant does business in the State of California and has annual gross revenues exceeding $25 million. Accordingly, Defendant is a "business" within the meaning of the Cal. Civ. Code § 1798.140(d) and is obligated to comply with the CCPA's requirements.

305. Pursuant to Cal. Civ. Code § 1798.150(b), counsel for Representative Plaintiffs served Defendant with notice of these CCPA violations by certified mail, return receipt requested.

306. On or about August 22, 2024, Defendant responded to this notice but its response demonstrated that it has not cured or is unable to "actually" cure the violation within the allotted 30 days. Consequently, Representative Plaintiffs seek all relief available under the CCPA including damages to be measured as the greater of actual damages or statutory damages in an amount from $100 up to $750 per consumer per incident. Cal. Civ. Code § 1798.150(a)(1)(A) & (b).

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

307. On behalf of California Subclass Members, Representative Plaintiffs also seek actual pecuniary damages and injunctive relief in the form of an order enjoining Defendant from continuing to violate the CCPA. Unless and until Defendant is restrained by order of the Court, its wrongful conduct will continue to cause irreparable injury to Representative Plaintiffs and the California Subclass.

308. As Defendant failed to timely rectify or otherwise cure the CCPA violations described herein, individually and on behalf of the California Subclass, Representative Plaintiffs seek statutory damages and any other relief the Court deems proper as a result of Defendant's CCPA violations pursuant to Cal. Civ. Code § 1798.150(a). In light of the serious conduct by Defendant, its past breaches (which put Defendant on notice to strengthen it cybersecurity practices), the persistence of Defendant's conduct, and its gross recklessness with Plaintiffs' and Subclass Members' PII, as described herein, Plaintiffs and the Class seek the maximum allowable statutory damages.

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

SIXTH CAUSE OF ACTION
Violation of the California Customer Records Act
Cal. Civ. Code §§ 1798.80, *et seq.*
(On Behalf of Plaintiffs and the California Subclass)

309. Representative Plaintiffs, individually and on behalf of the Subclass, incorporate by reference each of the factual allegations contained in the preceding paragraphs as if fully set forth herein.

310. "[T]o ensure that personal information about California residents is protected," the California legislature enacted Cal. Civ. Code § 1798.81.5, which requires that any business that "owns, licenses, or maintains personal information about a California resident shall implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure."

311. Defendant is a business that owns, maintains, or licenses personal information, within the meaning of Cal. Civ. Code § 1798.81.5, about Representative Plaintiffs and California Subclass members.

312. Defendant violated Cal. Civ. Code § 1798.81.5 by failing to implement reasonable measures to protect California Subclass members' PII.

313. Businesses that own or license computerized data that includes personal information are required to notify California residents when their PII has been acquired (or has reasonably believed to have been acquired) by unauthorized persons in a data security breach "in the most expedient time possible and without unreasonable delay." Cal. Civ. Code § 1798.82. Among other requirements, the security breach notification must include "the types of personal information that were or are reasonably believed to have been the subject of the breach." Cal. Civ. Code § 1798.82.

314. Defendant is a business that owns or licenses computerized data that includes personal information as defined by Cal. Civ. Code § 1798.82.

315. Representative Plaintiffs and California Subclass Members' PII includes personal information identified in Cal. Civ. Code § 1798.82(h) such as their names, Social Security numbers, driver's license numbers, and financial information, and is thereby covered by Cal. Civ. Code § 1798.82.

316. Representative Plaintiffs and the California Subclass Members are "customers" within the meaning of Cal. Civ. Code § 1798.80(c), as their personal information was provided to Defendant for the purpose of obtaining services or products.

317. The Data Breach constituted a breach of Defendant's security systems, networks and servers.

318. Because Defendant reasonably believed that Representative Plaintiffs and California Subclass Members' PII was acquired by unauthorized persons during the Data Breach, Defendant had an obligation to disclose the data breach in a timely and accurate fashion as mandated by Cal. Civ. Code § 1798.82.

319. Defendant unreasonably delayed informing Representative Plaintiffs and the California Subclass Members about the breach of security of their PII after it knew the breach had occurred. As a result of this unreasonable delay, Representative Plaintiffs and class members were

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

harmed separately and independently of the Data Breach itself because they were prevented from taking timely steps to mitigate their own damages and, thus, also suffered an incremental harm.

320. Upon information and belief, no law enforcement agency instructed Defendant that notification to California Subclass Members would impede an investigation.

321. Thus, by failing to disclose the Data Breach in a timely and accurate manner, the Defendant also violated Cal. Civ. Code § 1798.82.

322. Pursuant to Cal. Civ. Code § 1798.84, "[a]ny waiver of a provision of this title is contrary to public policy and is void and unenforceable," "[a]ny customer injured by a violation of this title may institute a civil action to recover damages," and "[a]ny business that violates, proposed to violate, or has violated this title may be enjoined."

323. As a direct and proximate result of Defendant's violations of Cal. Civ. Code §§ 1798.81.5 and 1798.82, Representative Plaintiffs and California Subclass Members were (and continue to be) injured and suffered (and will continue to suffer) damages, as described above.

324. Representative Plaintiffs and California Subclass Members seek relief under Cal. Civ. Code § 1798.84, including, but not limited to, actual damages, any applicable statutory damages and equitable and injunctive relief.

RELIEF SOUGHT

WHEREFORE, Representative Plaintiffs, on Representative Plaintiffs' own behalf and on behalf of each member of the proposed Classes, respectfully requests that the Court enter judgment in Representative Plaintiffs' favor and for the following specific relief against Defendant (and/or each of them) 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 California Code of Civil Procedure § 382, including appointment of Representative Plaintiffs' counsel as Class Counsel;

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

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

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

4. That the Court enjoin Defendant, ordering it to cease and desist from unlawful activities in further violation of California Business and Professions Code §17200, *et seq.*;

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

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

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

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

c. requiring Defendant to delete and purge Representative Plaintiffs' and Class Members' Private Information unless Defendant can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Representative Plaintiffs and Class Members;

d. requiring Defendant to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of Representative Plaintiffs' and Class Members' Private Information;

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

f. prohibiting Defendant from maintaining Representative Plaintiffs' and Class Members' Private Information 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 security checks;

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

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 Plaintiffs 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; 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.

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

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

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

JURY DEMAND

Representative Plaintiffs, individually and on behalf of the Plaintiff Class, hereby demand a trial by jury for all issues triable by jury.

Dated: October 4, 2024

Scott Edward Cole, Esq. (S.B. #160744)
Alicyn B. Whitley, Esq. (S.B. #325927)
COLE & VAN NOTE
555 12th Street, Suite 2100
Oakland, California 94607
Telephone: (510) 891-9800
Email: sec@colevannote.com
Email: abw@colevannote.com

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

M. Anderson Berry, Esq. (S.B. #262879)
Gregory Haroutunian, Esq. (S.B. #330263)
Brandon P. Jack, Esq. (S.B. #325584)
CLAYEO C. ARNOLD
A PROFESSIONAL CORPORATION
865 Howe Avenue
Sacramento, CA 95825
Telephone: (916) 239-4778
Email: aberry@justice4you.com
Email: gharoutunian@justice4you.com
Email: bjack@justice4you.com

Robert C. Schubert, Esq. (S.B. #62684)
Amber L. Schubert, Esq. (S.B. #278696)
SCHUBERT JONCKHEER & KOLBE LLP
2001 Union Street, Suite 200
San Francisco, CA 94123
Telephone: (415) 788-4220
Email: rschubert@sjk.law
Email: aschubert@sjk.law

Interim Co-Lead Class Counsel

Sabita J. Soneji, Esq. (S.B. #224262)
TYCKO & ZAVAREEI LLP
1970 Broadway, Suite 1070
Oakland, CA 94612
Telephone: (510) 254-6808
Email: ssoneji@tzlegal.com

Rachele R. Byrd, Esq. (S.B. #190634)
Alex J. Tramontano, Esq. (S.B. #276666)
WOLF HALDENSTEIN ADLER
FREEMAN & HERZ LLP
750 B Street, Suite 1820
San Diego, CA 92101
Telephone: (619) 239-4599
Email: byrd@whafh.com
Email: tramontano@whafh.com

Plaintiffs' Executive Committee Members

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