KAZEROUNI LAW GROUP, APC
Abbas Kazerounian, Esq. (SBN 249203)
ak@kazlg.com
Mona Amini (SBN 296829)
mona@kazlg.com
245 Fischer Avenue, Unit D1
Costa Mesa, California 92626
Telephone: (800) 400-6808
Facsimile: (800) 520-5523

BLOOD HURST & O'REARDON, LLP
Timothy G. Blood, Esq. (SBN 149343)
tblood@bholaw.com
Jennifer L. MacPherson, Esq. (SBN 202021)
jmacpherson@bholaw.com
501 West Broadway, Suite 1490
San Diego, CA 92101
Telephone: (619) 338-1100
Facsimile: (619) 338-1101

MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN, PLLC
DAVID K. LIETZ (*PHV forthcoming*)
5335 Wisconsin Avenue NW, Suite 440
Washington, DC 20015-2052
dlietz@milberg.com

WOLF HALDENSTEIN ADLER FREEMAN & HERZ LLP
Rachele R. Byrd (SBN 190634)
byrd@whafh.com
750 B Street, Suite 1820
San Diego, California
Telephone: (619) 239-4599
Facsimile: (619) 234-4599

CLAYEO C. ARNOLD, APC
M. Anderson Berry (SBN 262879)
aberry@justice4you.com
865 Howe Avenue
Sacramento, CA 95825
Telephone: (916) 777-7777
Facsimile: (916) 924-1829

Attorneys for Plaintiffs and the Proposed Class
[additional counsel appear on signature page]

SUPERIOR COURT OF THE STATE OF CALIFORNIA

FOR THE COUNTY OF SAN DIEGO – COMPLEX CIVIL

IVO KOLAR and MICHAEL MILLER, individually, and on behalf of all others similarly situated,

Plaintiffs,

vs.

CSI FINANCIAL SERVICES LLC dba CLEARBALANCE, a Nevada corporation; and DOES 1-50, inclusive,

Defendant(s).

Case No.: 37-2021-00030426-CU-NP-CTL

SECOND AMENDED CLASS ACTION COMPLAINT FOR VIOLATIONS OF:

1. CALIFORNIA CONSUMER PRIVACY ACT OF 2018, CAL. CIV. CODE §§ 1798.100, *et seq.*;
2. CALIFORNIA CONFIDENTIALITY OF MEDICAL INFORMATION ACT, CAL. CIV. CODE §§ 56, *et seq.*;
3. CALIFORNIA UNFAIR COMPETITION LAW, CAL. BUS. & PROF. CODE §§ 17200, *et. seq.*; and
4. BREACH OF CONTRACT

JURY TRIAL DEMANDED

Plaintiffs Ivo Kolar and Michael Miller, Ronald Maloney, Travis Holmes, Scott Moore, Joseph Franklin, and Brooke Roberts-Gooden ("Plaintiffs"), individually and on behalf of the general public and all others similarly situated (the "Class members"), by and through their attorneys, upon personal knowledge as to facts pertaining to themselves and on information and belief as to all other matters, bring this class action against CSI Financial Services LLC dba ClearBalance and DOES 1-50, inclusive ("Defendant"), and allege as follows:

NATURE OF THE CASE

1. This is a data breach class action arising out of Defendant's failure to implement and maintain reasonable security practices to protect consumers' sensitive personal information. Defendant is a financing company which provides patient financing programs to U.S. hospitals and health care systems. Defendant has "served more than 4 million patient accounts at hundreds of healthcare organizations nationwide."[1] For its business purposes, Defendant obtains, stores, and transmits personally identifiable information ("PII") and protected health information ("PHI") from customers like Plaintiffs, including but not limited to its customers' names, addresses, driver's license numbers, Social Security numbers, tax identification numbers, dates of birth, telephone numbers, healthcare account numbers and balances, personal banking information (financial institution names, account numbers, and routing numbers), health insurance information, clinical information and full face images of its customers.

2. On April 26, 2021, Defendant became of aware of an attempted unauthorized transfer of ClearBalance funds. Defendant engaged a forensic investigator, and during the investigation, Defendant learned that unauthorized users had accessed ClearBalance email accounts between March 8, 2021 and April 26, 2021. On June 21, 2021, Defendant also learned that unauthorized persons accessed ClearBalance emails that contained individuals' personal information, including: name, tax ID, Social Security number, date of birth, other government-issued ID, telephone number, healthcare account number and balance, date of service, ClearBalance loan number and balance, personal banking information, clinical information, health insurance information, and full-face photographic

[1] https://www.myclearbalance.com/About.

image (the "Data Breach"). Although the exact number of affected customers is presently unknown, based upon information and belief at least 209,719 customers[2] have been affected by the Data Breach, including 14,950 residents of California. The Data Breach occurred between March 8, 2021 and April 26, 2021. However, Defendant only provided notice to Plaintiffs and its other customers of the Data Breach on or around July 9, 2021.

3. Although Defendant knew about the Data Breach and that sensitive customer information was in the hands of malicious actors, it waited until July 9, 2021, to send certain customers letters regarding the Data Breach. Defendant's notice to customers was misleading and inadequate as the notice did not explain the two-month delay between discovering the breach and notifying affected customers.

4. The Data Breach happened as a result of Defendant's inadequate cybersecurity, which caused Plaintiffs' and the Class members' PII/PHI to be accessed, exfiltrated, and disclosed to unauthorized persons. This action seeks to remedy these failings. Plaintiffs bring this action on behalf of themselves and all affected U.S. residents.

5. As set forth in the Prayer for Relief, among other things, Plaintiffs seek, for themselves and the Class injunctive relief, including public injunctive relief, and actual damages.

VENUE AND JURISDICTION

6. This Court has jurisdiction over this action pursuant to Cal. Code Civ. Proc. § 410.10 and Cal. Bus. & Prof. Code §§ 17203-17204, 17604. This action is brought as a class action on behalf of Plaintiffs and the Class members pursuant to Cal. Code Civ. Proc. § 382.

7. This Court has personal jurisdiction over Defendant because Defendant regularly conducts business in California and is headquartered in San Diego, California.

8. Venue is proper in this Court pursuant to Cal. Code Civ. Proc. § 395 and § 395.5 because Defendant regularly conducts business in the State of California, Defendant is headquartered

[2] Defendant reported to the Office of the Maine Attorney General that 209,719 persons were affected by the Data Breach. *See* https://apps.web.maine.gov/online/aeviewer/ME/40/10900d6e-0624-4c2f-a58a-6a1b6b798091.shtml.

in San Diego, California, and the unlawful acts or omissions giving rise to this action also occurred or arose in this county.

PARTIES

9. At all relevant times, Plaintiff Ivo Kolar resided in the State of California.

10. At all relevant times, Plaintiff Michael Miller resided in the State of California.

11. At all relevant times, Plaintiff Brooke Roberts-Gooden resided in the State of North Carolina.

12. At all relevant times, Plaintiff Ronald Maloney resided in the State of Texas.

13. At all relevant times, Plaintiff Travis Holmes resided in the State of Florida.

14. At all relevant times, Plaintiff Scott Moore resided in the State of Ohio.

15. At all relevant times, Plaintiff Joseph Franklin resided in the State of Texas.

16. At all relevant times, Defendant conducted business in the State of California.

17. Plaintiffs each provided their PII/PHI to Defendant as part of financing their medical expenses, including Plaintiffs' names, Social Security numbers, health insurance information, addresses, telephone numbers, and personal banking information, including account numbers and routing numbers. In July 2020, Plaintiffs were notified that their PII/PHI was accessed by unauthorized individuals through the Data Breach.

18. Defendant sent Plaintiffs a letter dated July 9, 2021 with the title, "Notice of Data Breach." The letter notified Plaintiffs and similarly situated persons that as a result of a "data security incident" a malicious actor had gained unauthorized access to certain PII/PHI in Defendant's email accounts and emails containing individuals' personal information, including: name, tax ID, Social Security number, date of birth, other government-issued ID, telephone number, healthcare account number and balance, date of service, ClearBalance loan number and balance, personal banking information, clinical information, health insurance information, and full-face photographic image. No details were provided regarding who stole the information or why there was a delay in notifying affected customers.

19. As a result of Defendant's failure to implement and maintain reasonable security procedures and practices appropriate to the nature of the personal information it collected, maintained,

and stored on its servers, network, and/or email system, Plaintiffs' PII/PHI was accessed, viewed, exfiltrated, stolen and/or otherwise disclosed to unauthorized persons in the Data Breach.

20. Defendant is a limited liability company formed under the laws of the State of Nevada and headquartered at 3636 Nobel Dr., Ste. 250, San Diego, California 92122. Defendant is a lender and/or loan servicer that offers loans and services loans made by hospitals and providers to patients in order to finance medical expenses.

21. Plaintiffs are unaware of the true names and capacities of the Defendant sued herein as DOES 1 through 50, inclusive, and therefore sue this Defendant by such fictitious names pursuant to Cal. Civ. Proc. Code § 474. Plaintiffs are informed and believe, and based thereon, allege that Defendant designated herein is legally responsible in some manner for the unlawful acts and occurrences complained of herein, whether such acts were committed intentionally, negligently, recklessly, or otherwise, and Defendant thereby proximately caused the injuries and damages to Plaintiffs and the Class members as herein alleged. Plaintiffs will seek leave of Court to amend this complaint to reflect the true names and capacities of Defendant when they have been ascertained and become known.

22. The agents, servants and/or employees of Defendant and each of them acting on behalf of Defendant acted within the course and scope of his, her or its authority as the agent, servant and/or employee of Defendant, and personally participated in the conduct alleged herein on behalf of Defendant with respect to the conduct alleged herein. Consequently, the acts of each Defendant are legally attributable to the other Defendants and all Defendants are jointly and severally liable to Plaintiffs and other similarly situated individuals, for the loss sustained as a proximate result of the conduct of the Defendants' agents, servants and/or employees.

/ / /

/ / /

/ / /

/ / /

/ / /

/ / /

FACTUAL ALLEGATIONS

PII/PHI Is a Valuable Property Right that Must Be Protected

23. The California Constitution guarantees every Californian a right to privacy. PII/PHI is a recognized valuable property right.[3] California has repeatedly recognized this property right, most recently with the passage of the California Consumer Privacy Act of 2018.

24. In a Federal Trade Commission ("FTC") roundtable presentation, former Commissioner, Pamela Jones Harbour, underscored the property value attributed to PII by observing:

> Most consumers cannot begin to comprehend the types and amount of information collected by businesses, or why their information may be commercially valuable. Data is currency. The larger the data set, the greater potential for analysis – and profit.[4]

25. The value of PII as a commodity is measurable. "PII, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets."[5] It is so valuable to identity thieves that once PII/PHI has been disclosed, criminals often trade it on the "cyber black-market" for several years.

26. Companies recognize PII as an extremely valuable commodity akin to a form of personal property. For example, Symantec Corporation's Norton brand has created a software application that values a person's identity on the black market.[6]

27. As a result of its real value and the recent large-scale data breaches, identity thieves and cyber criminals openly post credit card numbers, Social Security numbers, PII and other sensitive information directly on various illicit Internet websites making the information publicly available for other criminals to take and use. This information from various breaches, including the information

---

[3] *See* John T. Soma, et al., *Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("PII") Equals the "Value" of Financial Assets*, 15 RICH. J.L. & TECH. 11, at *2 (2009) ("PII, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets.") (citations omitted).

[4] FTC, *Statement of FTC Commissioner Pamela Jones Harbour* (Remarks Before FTC Exploring Privacy Roundtable) (Dec. 7, 2009), https://www.ftc.gov/public-statements/2009/12/remarks-ftc-exploring-privacy-roundtable.

[5] *See* Soma, *Corporate Privacy Trend, supra*.

[6] Risk Assessment Tool, Norton 2010, www.everyclickmatters.com/victim/assessmenttool.html.

exposed in the Data Breach, can be aggregated and become more valuable to thieves and more damaging to victims. In one study, researchers found hundreds of websites displaying stolen PII and other sensitive information. Strikingly, none of these websites were blocked by Google's safeguard filtering mechanism – the "Safe Browsing list."

28. PHI is particularly valuable. All-inclusive health insurance dossiers containing sensitive health insurance information, names, addresses, telephone numbers, email addresses, Social Security numbers and bank account information, complete with account and routing numbers, can fetch up to $1,200 to $1,300 each on the black market.[7] According to a report released by the Federal Bureau of Investigation's ("FBI") Cyber Division, criminals can sell healthcare records for 50 times the price of a stolen Social Security or credit card number.[8]

29. Recognizing the high value that consumers place on their PII/PHI, some companies now offer consumers an opportunity to sell this information to advertisers and other third parties. The idea is to give consumers more power and control over the type of information they share – and who ultimately receives that information. By making the transaction transparent, consumers will make a profit from the surrender of their PII/PHI.[9] This business has created a new market for the sale and purchase of this valuable data.[10]

30. Consumers place a high value not only on their PII/PHI, but also on the privacy of that data. Researchers shed light on how much consumers value their data privacy – and the amount is considerable. Indeed, studies confirm that "when privacy information is made more salient and

---

[7] Adam Greenberg, *Health Insurance Credentials Fetch High Prices in the Online Black Market* (July 16, 2013), *available at* https://www.scmagazine.com/home/security-news/health-insurance-credentials-fetch-high-prices-in-the-online-black-market/.

[8] Federal Bureau of Investigation, *Health Care Systems and Medical Devices at Risk for Increased Cyber Intrusions for Financial Gain* (April 8, 2014) *available at* https://www.illuminweb.com/wp-content/uploads/ill-mo-uploads/103/2418/health-systems-cyber-intrusions.pdf.

[9] Steve Lohr, *You Want My Personal Data? Reward Me for It*, N.Y. Times (July 16, 2010) *available at* https://www.nytimes.com/2010/07/18/business/18unboxed.html.

[10] *See* Julia Angwin and Emil Steel, *Web's Hot New Commodity: Privacy*, Wall Street Journal (Feb. 28, 2011) *available at* https://www.wsj.com/articles/SB10001424052748703529004576160764037920274.

accessible, some consumers are willing to pay a premium to purchase from privacy protective websites."[11]

31. One study on website privacy determined that U.S. consumers valued the restriction of improper access to their PII between $11.33 and $16.58 per website.[12]

32. Given these facts, any company that transacts business with a consumer and then compromises the privacy of consumers' PII/PHI has thus deprived that consumer of the full monetary value of the consumer's transaction with the company.

Theft of PII/PHI Has Grave and Lasting Consequences for Victims

33. A data breach is an incident in which sensitive, protected, or confidential data has potentially been viewed, stolen, or used by an individual unauthorized to do so. As more consumers rely on the internet and apps on their phone and other devices to conduct every-day transactions, data breaches are becoming increasingly more harmful.

34. Theft or breach of PII/PHI is serious. The California Attorney General recognizes that "[f]oundational" to every Californian's constitutional right to privacy is "information security: if companies collect consumers' personal data, they have a duty to secure it. An organization cannot protect people's privacy without being able to secure their data from unauthorized access."[13]

35. The United States Government Accountability Office noted in a June 2007 report on Data Breaches ("GAO Report") that identity thieves use PII to take over existing financial accounts, open new financial accounts, receive government benefits and incur charges and credit in a person's name.[14] As the GAO Report states, this type of identity theft is so harmful because it may take time for the victim to become aware of the theft and can adversely impact the victim's credit rating.

---

[11] Janice Y. Tsai, et al., *The Effect of Online Privacy Information on Purchasing Behavior, An Experimental Study Information Systems Research* 22(2) 254, 254 (June 2011), *available at* https://www.jstor.org/stable/23015560?seq=1#page_scan_tab_contents.

[12] II–Horn, Hann, et al., *The Value of Online Information Privacy: An Empirical Investigation* (Mar. 2003) at table 3, *available at* https://ideas.repec.org/p/wpa/wuwpio/0304001.html.

[13] California Data Breach Report, Kamala D. Harris, Attorney General, California Department of Justice, February 2016.

[14] *See* GAO, GAO Report 9 (2007), *available at* http:///www.gao.gov/new.items/d07737.pdf.

36. In addition, the GAO Report states that victims of identity theft will face "substantial costs and inconveniences repairing damage to their credit records … [and their] good name." According to the FTC, identity theft victims must spend countless hours and large amounts of money repairing the impact to their good name and credit record.[15]

37. Identity thieves use personal information for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud.[16] According to Experian, "[t]he research shows that personal information is valuable to identity thieves, and if they can get access to it, they will use it" to among other things: open a new credit card or loan; change a billing address so the victim no longer receives bills; open new utilities; obtain a mobile phone; open a bank account and write bad checks; use a debit card number to withdraw funds; obtain a new driver license or ID; use the victim's information in the event of arrest or court action.[17]

38. According to the IBM and Ponemon Institute's 2019 "Cost of a Data Breach" report, the average cost of a data breach per consumer was $150 per record.[18] Other estimates have placed the costs even higher. The 2013 Norton Report estimated that the average cost per victim of identity theft – a common result of data breaches – was $298 dollars.[19] And in 2019, Javelin Strategy &

---

[15] *See* FTC Identity Theft Website: https://www.consumer.ftc.gov/features/feature-0014-identity-theft.

[16] The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority." 16 C.F.R. § 603.2. The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other 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." *Id*.

[17] *See* Susan Henson, *What Can Identity Thieves Do with Your Personal Information and How Can You Protect Yourself?*, EXPERIAN (Sept. 7, 2017), *available at* https://www.experian.com/blogs/ask-experian/what-can-identity-thieves-do-with-your-personal-information-and-how-can-you-protect-yourself/.

[18] Brook, *What's the Cost of a Data Breach in 2019, supra*.

[19] Norton By Symantec, 2013 Norton Report 8 (2013), *available at* https://yle.fi/tvuutiset/uutiset/upics/liitetiedostot/norton_raportti.pdf.

Research compiled consumer complaints from the FTC and indicated that the median out-of-pocket cost to consumers for identity theft was $375.[20]

39. The consequences can be even more serious when the hack includes taking PHI. Data breaches involving medical information "typically leave[] a trail of falsified information in medical records that can plague victims' medical and financial lives for years."[21] It "is also more difficult to detect, taking almost twice as long as normal identity theft."[22] "A thief may use your name or health insurance numbers to see a doctor, get prescription drugs, file claims with your insurance provider, or get other care. If the thief's health information is mixed with yours, your treatment, insurance and payment records, and credit report may be affected."[23]

40. Further, medical data is more valuable than other commonly available personal data. "While a stolen credit card number might be sold for just a few cents, medical files can be worth as much as $1,000 each" or more.[24]

41. A report published by the World Privacy Forum and presented at the U.S. FTC Workshop on Informational Injury describes what medical identity theft victims may experience:

- Changes to their health care records, most often the addition of falsified information, through improper billing activity or activity by imposters. These changes can affect the healthcare a person receives if the errors are not caught and corrected.
- Significant bills for medical goods and services not sought nor received.
- Issues with insurance, co-pays, and insurance caps.
- Long-term credit problems based on problems with debt collectors reporting debt due to identity theft.

---

[20] Facts + Statistics: *Identity Theft and Cybercrime*, Insurance Information Institute, *available at* https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime (citing the Javelin report).

[21] Pam Dixon, et al., *The Geography of Medical Identity Theft* (Dec. 12, 2017), https://www.ftc.gov/system/files/documents/public_comments/2018/01/00037-142815.pdf.

[22] *See* FBI CYBER DIVISION, (U) HEALTH CARE SYSTEMS AND MEDICAL DEVICES AT RISK FOR INCREASED CYBER INTRUSIONS FOR FINANCIAL GAIN 2 (2014), *available at* https://publicintelligence.net/fbi-health-care-cyber-intrusions/ (FBI, April 8, 2014).

[23] *See* Federal Trade Commission, *Medical Identity Theft*, *available at* http://www.consumer.ftc.gov/articles/0171-medical-identity-theft.

[24] Brian O'Connor, *Healthcare Data Breach: What to Know About Them and What to Do After One*, Experian (June 14, 2018), https://www.experian.com/blogs/ask-experian/healthcare-data-breach-what-to-know-about-them-and-what-to-do-after-one/.

- Serious life consequences resulting from the crime; for example, victims have been falsely accused of being drug users based on falsified entries to their medical files; victims have had their children removed from them due to medical activities of the imposter; victims have been denied jobs due to incorrect information placed in their health files due to the crime.
- As a result of improper and/or fraudulent medical debt reporting, victims may not qualify for mortgage or other loans and may experience other financial impacts.
- Phantom medical debt collection based on medical billing or other identity information.
- Sales of medical debt arising from identity theft can perpetuate a victim's debt collection and credit problems, through no fault of their own.

42. A person whose PII/PHI has been compromised may not see any signs of identity theft for years. According to the GAO Report:

> [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.

43. For example, in 2012, hackers gained access to LinkedIn's users' passwords. However, it was not until May 2016, four years after the breach, that hackers released the stolen email and password combinations.[25]

44. It is within this context that Plaintiffs and over 200,000 of Defendant's customers face imminent risk of identity theft and must now live with the knowledge that their PII/PHI is forever in cyberspace and was taken, accessed, and viewed by unauthorized persons willing and able to use the information for any number of improper purposes and scams, including making the information available for sale on the dark web or the black market.

Defendant's Businesses

45. Defendant is a lender and loan-servicing company that provides patient financing programs to hospitals and other healthcare facilities across the country.

46. When Plaintiffs and similarly situated customers apply for financing with or through Defendant, they are required to provide Defendant with certain personal information. This personal

---

[25] *See* Cory Scott, *Protecting Our Members*, LINKEDIN (May 18, 2016), *available at* https://blog.linkedin.com/2016/05/18/protecting-our-members.

information includes the customer's name, Social Security number, date of birth, driver's license and/or other government issued ID containing a photograph, telephone number, healthcare account number, personal bank account information, and health insurance information. Plaintiffs reasonably believed that Defendant would keep their PII/PHI secure.

Defendant's Collection of Customers' PII/PHI

47. Defendant acknowledges that it obtains, stores and transmits a substantial amount of personal, financial, and medical information from its customers. The type of information is detailed in Defendant's Privacy Policy (last updated January 2020),[26] which states that Defendant collects the following categories of personal information from customers:

- Name, address, billing address, telephone number(s), email address, Social Security number, date of birth, financial account number(s), and credit card and debit card information, and information about customer's online activity.

48. Defendant collects personal information from customers that they voluntarily provide in various ways, including when customers obtain financing through Defendant or their loan is serviced by Defendant.

49. For California customers, Defendant's Privacy Policy identifies the rights of California residents regarding their personal information pursuant to the California Consumer Privacy Act ("CCPA").[27] These rights include requesting disclosure of the information collected, the purpose for collecting the information, and any third parties with whom the information is sold or disclosed. Additionally, the rights under the CCPA identified by Defendant's Privacy Policy include requesting deletion of the personal information, opting out of have personal information sold to third parties, and receiving information that identifies any third party that has received personal information.

50. The CCPA Privacy Policy sets forth the categories of personal information Defendant collects. This includes the following: identifiers (e.g., alias, postal address, unique personal identifier, online identifier, Internet Protocol address, email address, account name, Social Security number, driver's license number, passport number); personal records (e.g., signature, telephone number,

---

[26] *See* Defendant's Privacy Policy, *available at* ttps://www.myclearbalance.com/About/Privacy.

[27] https://www.myclearbalance.com/About/CAPrivacy.

hospital account number, insurance policy number, bank account number, credit card number, debit card number, or any other financial information medical information, or health insurance information); consumer characteristics (e.g., marital status, religion, military status, familial status, race, disability, gender identity, and creed); internet usage information (e.g., browsing history, search history, and information regarding your interaction with an Internet Web site, application, or advertisement); sensory data (audio recordings of customer care calls, electronic, visual, thermal, olfactory, or similar information); geolocation data; professional or employment information (e.g., profession, employment history); commercial information (e.g. personal property, purchasing or consuming history); inferences from personal information collected (e.g., your preferences, your likelihood of interest in certain of our services).

Defendant's Promises to Safeguard Customer PII/PHI

51. Defendant promises that it "respect(s) the privacy of our customers and are committed to protecting their information on our websites with the same care we use for all ClearBalance® transactions."[28]

52. Defendant claims it uses "industry standard physical, technical and administrative security measures and safeguards to protect the confidentiality and security of your personal information."[29]

53. Defendant warns that "since the Internet is not a 100 percent secure environment, we cannot guarantee, ensure, or warrant the security of any information you transmit to us. There is no guarantee that information may not be accessed, disclosed, altered, or destroyed by breach of any of our physical, technical, or managerial safeguards. It is your responsibility to protect the security of your login information."

54. Defendant's Terms of Use expressly references Defendant's Privacy Policy.

The Data Breach

55. On July 9, 2021, Defendant sent Plaintiffs and other similarly situated customers a letter with the title, "Notice of Data Breach." The letter states that "CSI Financial Services LLC

---

[28] https://www.myclearbalance.com/About/Privacy.

[29] *Id*.

("ClearBalance") writes to inform you of a data security incident at ClearBalance that involved some of your personal information."

56. The letter goes on to state that Defendant "detected and prevented unauthorized wire transfer of ClearBalance funds" on April 26, 2021, and that "there was unauthorized access to certain ClearBalance email accounts between March 8, 2021 and April 26, 2021."

57. Further, the letter states that on "June 21, 2021, our investigation also determined that there was unauthorized access to emails that contained personal information related to certain individuals participating in the ClearBalance program, including you."

58. According to Defendant, the information in the Data Breach included Plaintiff Ivo Kolar's name, Social Security number, date of birth, telephone number, ClearBalance loan number and balance.

59. According to Defendant, the information in the Data Breach included Plaintiff Michael Miller's name, Social Security number, date of birth, telephone number, and ClearBalance loan number and balance.

60. Defendant also claimed to have immediately launched its own investigation after the April 26, 2021, security incident.

61. Defendant offered customers a two year complimentary membership to IDX's identity theft program.

62. Additionally, Defendant offered a limited number of steps on how to protect against identity theft and fraud. These steps included reviewing financial account statements and credit reports.

63. For California residents, the letter does not identify the rights of consumers under CCPA and instead says to "[v]isit the California Office of Privacy Protection (www.oag.ca.gov/privacy) for additional information on protection against identity theft."

Defendant's Notice of Data Breach

64. On or around July 9, 2021, Defendant sent Plaintiffs and other similarly situated customers affected by the Data Breach the "Notice of Data Breach" letter.

65. Pursuant to California Civ. Code § 1798.82(a)(1), data breach notification letters must be sent to residents of California "whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person" due to a "breach of the security of the system[.]"

66. Plaintiffs' and the Class members' PII/PHI is "personal information" as defined by California Civ. Code § 1798.82(h).

67. California Civ. Code § 1798.82(g) defines "breach of the security of the system" as the "unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by the person or business."

68. The Data Breach was a "breach of the security of the system" as defined by California Civ. Code § 1798.82(g).

69. Thus, Defendant filed and disseminated its breach notification because Plaintiffs' and the Class members' unencrypted personal information was accessed and viewed by an unauthorized person or persons as a result of the Data Breach.

70. Defendant's Notice of the Data Breach letter sent to Plaintiffs and other putative Class members is inadequate and fails to provide sufficient detail. Defendant states only that it had "detected and prevented an attempted unauthorized wire transfer" on April 26, 2021 and that through its investigation it determined that "there was unauthorized access to certain ClearBalance email accounts between March 8, 2021, to April 26, 2021," and "[o]n June 21, 2021, [] [its] investigation also determined that there was unauthorized access to emails that contained personal information related to certain individuals participating in the ClearBalance program[.]" It is unclear whether the intrusion, or intrusions, occurred on two consecutive days or two separate days or every day. It also fails to indicate whether the breach was only of existing customer PII/PHI or whether it also included PII/PHI collected from former and/or potential customers.

71. Defendant's vague description of the Data Breach leaves Plaintiffs and Class members at continuing risk. By failing to adequately inform Plaintiffs and Class members of the details surrounding the breach Plaintiffs and Class members are unable to adequately protect themselves against identity theft and other damages.

72. Further, Defendant offered Plaintiffs and Class members little to assist them with any fall-out from the Data Breach or to advise them of the extent of the potential threat they face as a result of their sensitive PII/PHI being in the hands of criminals. Defendant's offer of a two year subscription to IDX's identity theft protection program is insufficient where Plaintiffs and Class members are now at increased risk of identity theft for years to come as a result of the Data Breach.

73. Defendant also fails to explain why it waited over two months to notify Plaintiffs and Class members about the Data Breach. This delayed Plaintiffs' and Class members' ability to take necessary precautions to protect themselves from identity theft and other fraud.

Defendant Knew or Should Have Known PII/PHI Are High Risk Targets

74. Defendant knew or should have known that PII and PHI like the information obtained, maintained and stored on Defendant's servers and network, including its email system, is a high risk target for identity thieves.

75. The Identity Theft Resource Center reported that the business sector had the largest number of breaches in 2018. According to the ITRC this sector suffered 571 data breaches exposing at least 415,233,143 records in 2018.[30] Further, the ITRC identified "hacking" as the most common form of data breach in 2018, accounting for 39% of data breaches.

76. Companies are increasingly being targeted with phishing attacks. A phishing attack is a method of infiltrating for the purpose of removing data for the purpose of viewing and using it to commit acts such as identity theft and otherwise wrongfully obtaining money or other things of value. Sometimes the person who engaged in phishing uses the data obtained to commit cyber fraud and sometimes the person sells the data to other identity thieves. Either way, the information must be viewed to be of any use or to confirm the contents of the data before being sold.

77. Phishing is a cybercrime in which a target or targets are contacted by email, telephone or text message by someone posing as a legitimate person or entity so that the recipient provides sensitive data. The hacker cannot do it by him or herself. A phishing incident requires the email

[30] Identity Theft Resource Center, *2018 End-of-Year Data Breach Report, available at* https://www.idtheftcenter.org/wp-content/uploads/2019/02/ITRC_2018-End-of-Year-Aftermath_FINAL_V2_combinedWEB.pdf.

system to allow the phishing email to reach the email recipient, for the email recipient to click on a link, provide login credentials, download a file, or take similar affirmative action to allow the hacker to compromise the email recipient's system. The information is then used to access important accounts such as Plaintiffs' and Class members' PII/PHI.

78. Phishing does not just happen. To be successful, phishing relies on a series of affirmative acts by a company and its employees. This is because computers must be told what to do; they do not make independent decisions. Rather, they rely on instructions and actions from users and programmers. A successful phishing attack also requires an intentional affirmative act on the part of, for example, a company employee, such as clicking a link, downloading a file, or providing sensitive information.

79. Phishing attempts are extremely common. According to the Anti-Phishing Working Group's ("APWG") Phishing Activity Trends Report for Q2 2020, the first half of the year saw 146,994 reported phishing attacks.[31] Verizon's 2020 Data Breach Investigation Report found that phishing is one of the top data breach threats, with 22 percent of data breaches involving phishing.

80. Phishing is one way identity thieves, scammers and fraudsters steal information. Comparitech explains the goal of phishing is to trick victims into divulging confidential or personal information that can then be used for fraudulent purposes, like identity theft.[32] The HIPAA Journal explains that phishing attacks on the healthcare industry typically have one of two objectives – to obtain access to PHI or to deliver ransomware. PHI is a valuable commodity on the black market because it can be used to create false identities, obtain free medical treatment, and commit insurance fraud. Thus, the goal of phishing is to obtain and use compromised data so that it may be used to commit fraud.[33]

81. The APWG describes phishing as a crime employing both social engineering and technical subterfuge to steal personal identity data and account credentials. Social engineering

---

[31] https://docs.apwg.org/reports/apwg_trends_report_q2_2020.pdf.

[32] https://www.comparitech.com/blog/information-security/common-phishing-scams-how-to-avoid/.

[33] https://www.hipaajournal.com/protect-healthcare-data-from-phishing/.

schemes prey on unwary victims by fooling them into believing they are dealing with a trusted, legitimate party, such as by using deceptive email addresses and email messages. Phishing schemes are designed to lead victims to counterfeit websites that trick recipients into divulging personal data such as usernames and passwords. Technical subterfuge schemes plant malware onto computers to steal credentials directly, often using systems that intercept victims' account usernames and passwords or misdirect victims to counterfeit websites.

82. The HIPAA Journal describes that most phishing attacks on the healthcare industry are deployed by email. The communications generally look authentic and instruct employees to follow a link to a web page – where they will be asked to complete some action that will trigger a malware download or enter their username and password to continue. In addition to ransomware, the malware may be in the form of surveillance software such as adware and keystroke loggers that can be downloaded to follow an employee's online activities and record their usernames and passwords. Other types of malicious software can be downloaded to create gateways for hackers to enter an organization's network remotely. If the phishing attempt has been successful in obtaining a username and password, the hacker will likely be able to access PHI almost immediately.[34]

83. Phishing attacks are successful when a company has not employed adequate security procedures such as (1) training employees on how to recognize and report phishing attacks and conducting mock phishing scenarios; (2) deploying spam filters that can be enabled to recognize and prevent emails from suspicious sources from ever reaching the inbox of employees; (3) keeping all systems current with the latest security patches and updates; (4) installing antivirus solutions and monitoring the antivirus status on all equipment; (5) developing a security policy that includes password expiration and complexity and using two factor authentication to prevent hackers who have compromised a user's credentials from ever gaining access; (6) encrypting all sensitive company information; (7) using only well-configured devices and employing good end point defenses that can stop malware from installing, even if a phishing email is clicked; and (8) implementing policies and procedures for responding quickly to incidents.

---

[34] *Id.*

84. Defendant negligently left its computer systems open to attack. Thus, once the unauthorized user gained access to ClearBalance email accounts, Defendant's email servers communicated—that is, disclosed—the contents of those accounts (including Plaintiffs' and Class members' PHI/PII) to the unauthorized person(s) for their use.

85. Prior to the Data Breach, there were many reports of high-profile data breaches that should have put a company like Defendant on high alert and forced it to closely examine its own security procedures, as well as those of third parties with which it did business and gave access to their subscriber PII/PHI.

86. In 2019, a record 1,473 data breaches occurred, resulting in approximately 164,683,455 sensitive records being exposed, a 17% increase from 2018. Of the 1,473 recorded data breaches, 525 of them, or 35.64%, were in the medical or healthcare industry. The 525 reported breaches reported in 2019 exposed nearly 40 million sensitive records (39,378,157), compared to only 369 breaches that exposed just over 10 million sensitive records (10,632,600) in 2018.

87. In light of recent high profile data breaches at other healthcare partner and provider companies, including, American Medical Collection Agency (25 million patients, March 2019) University of Washington Medicine (974,000 patients, December 2018), Florida Orthopedic Institute (640,000 patients, July 2020), Wolverine Solutions Group (600,000 patients, September 2018), Oregon Department of Human Services (645,000 patients, March 2019), Elite Emergency Physicians (550,000 patients, June 2020), Magellan Health (365,000 patients, April 2020), BJC Health System (286,876 patients, March 2020), Defendant knew or should have known that its electronic records would be targeted by cybercriminals.

88. As such, Defendant was aware that PII/PHI is at high risk of theft, and consequently should have but did not take appropriate and standard measures to protect Plaintiffs' and Class members' PII/PHI against cyber-security attacks that Defendant should have anticipated and guarded against, including phishing.

CLASS DEFINITION AND ALLEGATIONS

89. Pursuant to Cal. Code Civ. Proc. § 382 and Cal. Civ. Code § 1781, Plaintiffs seek to represent and intend to certify the following nationwide class:

> All persons to whom ClearBalance sent on or about July 9, 2021 a Notification Letter with the subject "Notice of Data Breach."

90. In addition to the nationwide Class defined above, Plaintiffs seek to represent a subclass ("California Sub-Class," collectively referred to with the above as the "Class") of approximately 14,950 Class Members who were California residents at the time of the Data Breach, defined as follows:

> All California residents, as confirmed by having a California address on file in Defendants' business records at the time of the Data Security Incident, whose personal identifying information ("PII") was subject to the Data Security Incident disclosed by Defendants on or about July 9, 2021.

91. Excluded from the Class are: (1) Defendant and its officers, directors, employees, principals, affiliated entities, controlling entities, agents, and other affiliates; (2) the agents, affiliates, legal representatives, heirs, attorneys at law, attorneys in fact, or assignees of such persons or entities described herein; and (3) the Judge(s) assigned to this case and any members of their immediate families.

92. Certification of Plaintiffs' claims for classwide treatment is appropriate because Plaintiffs can prove the elements of their claims on a classwide basis using the same evidence as would be used to prove those elements in individual actions alleging the same claims.

93. The Class members are so numerous and geographically dispersed throughout California that joinder of all Class members would be impracticable. The Class includes approximately 209,664 customers, including 14,950 Sub-Class members, including Plaintiffs and Class members. Plaintiffs therefore believe that the Class is so numerous that joinder of all members is impractical.

94. Plaintiffs' claims are typical of the claims of the Class. Plaintiffs, like all proposed members of the Class, had their PII/PHI compromised in the Data Breach. Plaintiffs and Class members were injured by the same wrongful acts, practices, and omissions committed by Defendant, as described herein. Plaintiffs' claims therefore arise from the same practices or course of conduct that give rise to the claims of all Class members.

95. There is a well-defined community of interest in the common questions of law and fact affecting Class members. The questions of law and fact common to Class members predominate over questions affecting only individual Class members, and include without limitation:

(a) Whether Defendant had a duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the PII/PHI it collected from Plaintiffs and Class members;

(b) Whether Defendant breached its duty to protect the PII/PHI of Plaintiffs and each Class member; and

(c) Whether Plaintiffs and each Class member are entitled to damages and other equitable relief.

96. Plaintiffs will fairly and adequately protect the interests of the Class members. Plaintiffs are each an adequate representative of the Class in that Plaintiffs have no interests adverse to or that conflict with the Class Plaintiffs seeks to represent. Plaintiffs have retained counsel with substantial experience and success in the prosecution of complex consumer protection class actions of this nature.

97. A class action is superior to any other available method for the fair and efficient adjudication of this controversy since individual joinder of all Class members is impractical. Furthermore, the expenses and burden of individual litigation would make it difficult or impossible for the individual members of the Class to redress the wrongs done to them, especially given that the damages or injuries suffered by each individual member of the Class are outweighed by the costs of suit. Even if the Class members could afford individualized litigation, the cost to the court system would be substantial and individual actions would also present the potential for inconsistent or contradictory judgments. By contrast, a class action presents fewer management difficulties and provides the benefits of single adjudication and comprehensive supervision by a single court.

98. Defendant has acted or refused to act on grounds generally applicable to the entire Class, thereby making it appropriate for this Court to grant final injunctive, including public injunctive relief, and declaratory relief with respect to the Class as a whole.

CAUSES OF ACTION

FIRST CAUSE OF ACTION
Violation of the California Consumer Privacy Act of 2018 ("CCPA")
(Cal. Civ. Code §§ 1798.100, *et seq.*)

99. Plaintiffs re-allege and incorporate by reference all proceeding paragraphs as if fully set forth herein.

100. As more personal information about consumers is collected by businesses, consumers' ability to properly protect and safeguard their privacy has decreased. Consumers entrust businesses with their personal information on the understanding that businesses will adequately protect it from unauthorized access and disclosure. The California Legislature explained: "The unauthorized disclosure of personal information and the loss of privacy can have devasting effects for individuals, ranging from financial fraud, identity theft, and unnecessary costs to personal time and finances, to destruction of property, harassment, reputational damage, emotional stress, and even potential physical harm."[35]

101. As a result, in 2018, the California Legislature passed the CCPA, giving consumers broad protections and rights intended to safeguard their personal information. Among other things, the CCPA imposes an affirmative duty on businesses that maintain personal information about California residents to implement and maintain reasonable security procedures and practices that are appropriate to the nature of the information collected. Defendant failed to implement such procedures which resulted in the Data Breach.

102. It also requires "[a] business that discloses personal information about a California resident pursuant to a contract with a nonaffiliated third party . . . [to] require by contract that the third party 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." Cal. Civ. Code § 1798.81.5(c).

---

[35] California Consumer Privacy Act (CCPA) Compliance, https://buyergenomics.com/ccpa-complience/.

103. Section 1798.150(a)(1) of the CCPA provides: "Any consumer whose nonencrypted or nonredacted personal information, as defined [by the CCPA] is subject to an unauthorized access and exfiltration, theft, or disclosure as a result of the business' violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information may institute a civil action for" statutory or actual damages, injunctive or declaratory relief, and any other relief the court deems proper.

104. Plaintiffs and the Class members are "consumer[s]" as defined by Civ. Code § 1798.140(g) because they are "natural person[s] who [are] California resident[s], as defined in Section 17014 of Title 18 of the California Code of Regulations, as that section read on September 1, 2017."

105. Defendant is a "business" as defined by Civ. Code § 1798.140(c) because Defendant:

a. is a "sole proprietorship, partnership, limited liability company, corporation, association, or other legal entity that is organized or operated for the profit or financial benefit of its shareholders or other owners";

b. "collects consumers' personal information, or on the behalf of which is collected and that alone, or jointly with others, determines the purposes and means of the processing of consumers' personal information";

c. does business in California; and

d. has annual gross revenues in excess of $25 million; or annually buys, receives for the business' commercial purposes, sells or shares for commercial purposes, alone or in combination, the personal information of 50,000 or more consumers, households, or devices; or derives 50 percent or more of its annual revenues from selling consumers' personal information.

106. The PII taken in the Data Breach is personal information as defined by Civil Code § 1798.81.5(d)(1)(A) because it contains Plaintiffs' and the Class members' unencrypted first and last names and Social Security number, among other information.

107. Plaintiffs' and the putative Class' PII was subject to unauthorized access and exfiltration, theft, or disclosure because their PII, including name, Social Security number, date of

birth, telephone number, ClearBalance loan number and balance was wrongfully taken, accessed, and viewed by unauthorized third parties.

108. The Data Breach occurred as a result of Defendant's failure to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect Plaintiffs' and the Class members' PII. Defendant failed to implement reasonable security procedures to prevent an attack on its server or network, including its email system, by hackers and to prevent unauthorized access of Plaintiffs' and the Class members' PII as a result of this attack.

109. On July 16, 2021, Plaintiff Ivo Kolar provided Defendant with written notice of its violations of the CCPA, pursuant to Civil Code § 1798.150(b)(1). On July 15, 2021, Plaintiff Michael Miller provided written notice to Defendant identifying the specific provisions of the CCPA he alleges Defendant has violated. Defendant has not cured the violation within 30 days thereof, therefore Plaintiffs are amending the complaint to also pursue the greater of statutory damages in an amount not less than one hundred dollars ($100) and not greater than seven hundred and fifty ($750) per consumer per incident, or actual damages, whichever is greater. *See* Cal. Civ. Code § 1798.150(a)(1)(A) & (b).

110. As a result of Defendant's failure to implement and maintain reasonable security procedures and practices that resulted in the Data Breach, Plaintiffs seek actual and statutory damages, injunctive relief, including public injunctive relief, declaratory relief, and any other relief as deemed appropriate by the Court.

SECOND CAUSE OF ACTION
Violation of the California Confidentiality of Medical Information Act ("CMIA")
(Cal. Civ. Code §§ 56, *et seq.*)

111. Plaintiffs re-allege and incorporate by reference all proceeding paragraphs as if fully set forth herein.

112. Section 56.10(a) of the California Civil Code provides that "[a] provider of health care, health care service plan, or contractor shall not disclose medical information regarding a patient of the provider of health care or an enrollee or subscriber of a health care service plan without first obtaining an authorization[.]"

113. Defendant is a "contractor" within the meaning of Civil Code § 56.05(d) and/or a "provider of healthcare" within the meaning of Civil Code § 56.06 and/or a "business organized for the purpose of maintaining medical information" and/or a "business that offers software or hardware to consumers . . . that is designed to maintain medical information" within the meaning of Civil Code § 56.06(a) and (b), and maintained and continues to maintain "medical information," within the meaning of Civil Code § 56.05(j), for "patients" of Defendant, within the meaning of Civil Code § 56.05(k).

114. Plaintiffs and all members of the Class are "patients" within the meaning of Civil Code § 56.05(k) and are "endanger[ed]" within the meaning of Civil Code § 56.05(e) because Plaintiffs and the Class fear that disclosure of their medical information could subject them to harassment or abuse.

115. Plaintiffs and the respective Class members, as patients, had their individually identifiable "medical information," within the meaning of Civil Code § 56.05(j), created, maintained, preserved, and stored on Defendant's computer network at the time of the breach.

116. Defendant, through inadequate security, allowed unauthorized third-party access to Plaintiffs' and each Class member's medical information, without the prior written authorization of Plaintiffs and the Class members, as required by Civil Code § 56.10 of the CMIA.

117. In violation of Civil Code § 56.10(a), Defendant disclosed Plaintiffs' and the Class members' medical information without first obtaining an authorization. Plaintiffs' and the Class members' medical information was viewed by unauthorized individuals as a direct and proximate result of Defendant's violation of Civil Code § 56.10(a).

118. In violation of Civil Code § 56.10(e), Defendant further disclosed Plaintiffs' and the Class members' medical information to persons or entities not engaged in providing direct health care services to Plaintiffs or the Class members or their providers of health care or health care service plans or insurers or self-insured employers.

119. Defendant violated Civil Code § 56.101 of the CMIA through its failure to maintain and preserve the confidentiality of the medical information of Plaintiffs and the Class.

120. In violation of Civil Code § 56.101(a), Defendant created, maintained, preserved, stored, abandoned, destroyed, or disposed of Plaintiffs' and the Class members' medical information

in a manner that failed to preserve and breached the confidentiality of the information contained therein. Plaintiffs' and the Class members' medical information was viewed by unauthorized individuals as a direct and proximate result of Defendant's violation of Civil Code § 56.101(a).

121. In violation of Civil Code § 56.101(a), Defendant negligently created, maintained, preserved, stored, abandoned, destroyed, or disposed of Plaintiffs' and the Class members' medical information. Plaintiffs' and the Class members' medical information was viewed by unauthorized individuals as a direct and proximate result of Defendant's violation of Civil Code § 56.101(a).

122. Plaintiffs' and the Class members' medical information that was the subject of the Data Breach included "electronic medical records" or "electronic health records" as referenced by Civil Code § 56.101(c) and defined by 42 U.S.C. § 17921(5).

123. In violation of Civil Code § 56.101(b)(1)(A), Defendant's electronic health record system or electronic medical record system failed to protect and preserve the integrity of electronic medical information. Plaintiffs' and the Class members' medical information was viewed by unauthorized individuals as a direct and proximate result of Defendant's violation of Civil Code § 56.101(b)(1)(A).

124. Defendant violated Civil Code § 56.36 of the CMIA through its failure to maintain and preserve the confidentiality of the medical information of Plaintiffs and the Class.

125. As a result of Defendant's above-described conduct, Plaintiffs and the Class have suffered damages from the unauthorized disclosure and release of their individual identifiable "medical information" made unlawful by Civil Code §§ 56.10, 56.101, 56.36.

126. As a direct and proximate result of Defendant's above-described wrongful actions, inaction, omissions, and want of ordinary care that directly and proximately caused the Data Breach, and violation of the CMIA, Plaintiffs and the Class members have suffered (and will continue to suffer) economic damages and other injury and actual harm in the form of, *inter alia*, (i) an imminent, immediate and the continuing increased risk of identity theft, identity fraud and medical fraud – risks justifying expenditures for protective and remedial services for which they are entitled to compensation, (ii) invasion of privacy, (iii) breach of the confidentiality of their PII/PHI, (iv) statutory damages under the California CMIA, (v) deprivation of the value of their PII/PHI, for

which there is a well-established national and international market, and/or (vi) the financial and temporal cost of monitoring their credit, monitoring their financial accounts, and mitigating their damages.

127. Plaintiffs, individually and for each member of the Class , seek nominal damages of one thousand dollars ($1,000) for each violation under Civil Code § 56.36(b)(1), and actual damages suffered, if any, pursuant to Civil Code § 56.36(b)(2), injunctive relief, as well as punitive damages of up to $3,000 per Plaintiff and each Class member, and attorneys' fees, litigation expenses and court costs, pursuant to Civil Code § 56.35.

THIRD CAUSE OF ACTION
Violation of the California Unfair Competition Law ("UCL")
(Cal. Bus. & Prof. Code §§ 17200, *et seq.*)

128. Plaintiffs re-allege and incorporate by reference all proceeding paragraphs as if fully set forth herein.

129. The UCL prohibits any "unlawful," "fraudulent" or "unfair" business act or practice and any false or misleading advertising, as those terms are defined by the UCL and relevant case law. By virtue of the above-described wrongful actions, inaction, omissions, and want of ordinary care that directly and proximately caused the Data Breach, Defendant engaged in unlawful, unfair and fraudulent practices within the meaning, and in violation of, the UCL.

130. In the course of conducting its business, Defendant committed "unlawful" business practices by, *inter alia*, knowingly failing to design, adopt, implement, control, direct, oversee, manage, monitor and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems to safeguard and protect Plaintiffs' and Class members' PII/PHI, and by violating the statutory and common law alleged herein, including, *inter alia*, California's Confidentiality of Medical Information Act (Civ. Code §§ 56.10(a), (e); 56.101(a), 56.101(b)(1)(A); 56.36), the California Consumer Privacy Act of 2018 (Cal. Civ. Code § 1798.150(a)(1)), the Health Insurance Portability and Accountability Act of 1996, (42 U.S.C. § 1302d; 45 C.F.R. §§ 164.306(a), (d), (e); 164.308(a); 164.312(a), (d), (e); 164.316(a), (b)), Civil Code § 1798.81.5, and Article I, Section 1 of the California Constitution (California's constitutional right to privacy). Plaintiffs and Class members reserve the right to allege other violations of law by

Defendant constituting other unlawful business acts or practices. Defendant's above-described wrongful actions, inaction, omissions, and want of ordinary care are ongoing and continue to this date.

131. Defendant also violated the UCL's unlawful prong by breaching contractual obligations created by its Privacy Policy and by knowingly and willfully or, in the alternative, negligently and materially violating Cal. Bus. & Prof. Code § 22576, which prohibits a commercial website operator from "knowingly and willfully" or "negligently and materially" failing to comply with the provisions of their posted privacy policy. Plaintiffs and Class members suffered injury in fact and lost money or property as a result of Defendant's violations of its Privacy Policy.

132. Defendant also violated the UCL by failing to adequately and timely notify Plaintiffs and Class members pursuant to Civil Code § 1798.82(a) regarding the unauthorized access and disclosure of their PII. If Plaintiffs and Class members had been adequately and timely notified in an appropriate fashion, they could have taken precautions to safeguard and protect their PII/PHI and identities.

133. Defendant's above-described wrongful actions, inaction, omissions, want of ordinary care, misrepresentations, practices, and non-disclosures also constitute "unfair" business acts and practices in violation of the UCL in that Defendant's wrongful conduct is substantially injurious to consumers, offends legislatively-declared public policy, and is immoral, unethical, oppressive, and unscrupulous. Defendant's practices are also contrary to legislatively declared and public policies that seek to protect PII/PHI and ensure that entities who solicit or are entrusted with personal data utilize appropriate security measures, as reflected by laws such as the CCPA, Article I, Section 1 of the California Constitution, and the FTC Act (15 U.S.C. § 45). The gravity of Defendant's wrongful conduct outweighs any alleged benefits attributable to such conduct. There were reasonably available alternatives to further Defendant's legitimate business interests other than engaging in the above-described wrongful conduct.

134. Plaintiffs and Class members suffered injury in fact and lost money or property as a result of Defendant's violations of its Privacy Policy and statutory and common law in that a portion of the money Plaintiffs and Class members paid for Defendant's products and services went to fulfill

the contractual obligations set forth in its Privacy Policy, including maintaining the security of their PII/PHI, and Defendant's legal obligations and Defendant failed to fulfill those obligations.

135. The UCL also prohibits any "fraudulent business act or practice." Defendant's above-described claims, nondisclosures and misleading statements were false, misleading and likely to deceive the consuming public in violation of the UCL.

136. As a direct and proximate result of Defendant's above-described wrongful actions, inaction, omissions, and want of ordinary care that directly and proximately caused the Data Breach and their violations of the UCL, Plaintiffs and Class members have suffered injury in fact and lost money or property as a result of Defendant's unfair and deceptive conduct. Such injury includes paying for a certain level of security for their PII/PHI but receiving a lower level, paying more for Defendant's products and services than they otherwise would have had they known Defendant was not providing the reasonable security represented in its Privacy Policy and as in conformance with its legal obligations. Defendant's security practices have economic value in that reasonable security practices reduce the risk of theft of customer's PII/PHI.

137. Plaintiffs and Class members have also suffered (and will continue to suffer) economic damages and other injury and actual harm in the form of, *inter alia*, (i) an imminent, immediate and the continuing increased risk of identity theft and identity fraud – risks justifying expenditures for protective and remedial services for which they are entitled to compensation, (ii) invasion of privacy, (iii) breach of the confidentiality of their PII/PHI, (iv) statutory damages under the CCPA, (v) deprivation of the value of their PII/PHI for which there is a well-established national and international market, and/or (vi) the financial and temporal cost of monitoring their credit, monitoring financial accounts, and mitigating damages.

138. Unless restrained and enjoined, Defendant will continue to engage in the above-described wrongful conduct and more data breaches will occur. Plaintiffs, therefore, on behalf of themselves, Class members, and the general public, also seek restitution and an injunction, including public injunctive relief prohibiting Defendant from continuing such wrongful conduct, and requiring Defendant to modify its corporate culture and design, adopt, implement, control, direct, oversee, manage, monitor and audit appropriate data security processes, controls, policies, procedures

protocols, and software and hardware systems to safeguard and protect the PII/PHI entrusted to it, as well as all other relief the Court deems appropriate, consistent with Bus. & Prof. Code § 17203.

FOURTH CAUSE OF ACTION
Breach of Contract

139. Plaintiffs re-allege and incorporate by reference all proceeding paragraphs as if fully set forth herein.

140. Plaintiffs and Class members entered into express contracts with Defendant as set forth in its Terms of Use and Privacy Policy that included Defendant's promise to protect nonpublic personal information given to Defendant or that Defendant gathered on its own, from disclosure, as set forth in Defendant's Privacy Policy, which was posted on its website.

141. Plaintiffs and Class members performed their obligations under the contracts when they provided their PII/PHI to Defendant in relation to their purchase of insurance products or services from Defendant.

142. By allowing unauthorized users to gain access to Plaintiffs' and Class members' PII/PHI through the Data Breach, Defendant breached these contractual obligations. As a result, Defendant failed to comply with its own policies, including its Privacy Policy, and applicable laws, regulations and industry standards for data security and protecting the confidentiality of PII/PHI. Defendant's breach of contract also violated California Business and Professions Code § 22576, which prohibits a commercial website operator from "knowingly and willfully" or "negligently and materially" failing to comply with the provisions of their posted privacy policy.

143. By failing to fulfill its contractual obligations under its Terms of Use and Privacy Policy, Defendant failed to confer on Plaintiffs and Class members the benefit of the bargain, causing them economic injury.

144. As a direct and proximate result of the Data Breach, Plaintiffs and Class members have been harmed and have suffered, and will continue to suffer, damages and injuries.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, on behalf of themselves individually and all members of the Class, respectfully request that (i) this action be certified as a class action, (ii) Plaintiffs each be

designated representatives of the certified class(es), and (iii) Plaintiffs' undersigned counsel be appointed as Class Counsel. Plaintiffs, on behalf of themselves and members of the Class further request that upon final trial or hearing, judgment be awarded against Defendant for:

(i) actual and punitive damages to be determined by the trier of fact;

(ii) statutory damages;

(iii) equitable relief, including restitution;

(iv) appropriate injunctive relief;

(v) attorneys' fees and litigation expenses under Code of Civil Procedure § 1021.5 and other applicable law;

(vi) costs of suit;

(vii) pre- and post-judgment interest at the highest legal rates applicable; and

(viii) any such other and further relief the Court deems just and proper.

DEMAND FOR JURY TRIAL

Plaintiffs, on behalf of themselves individually and the putative Class, hereby demand a jury trial on all issues so triable.

Respectfully submitted,

Dated: April 22, 2022

BLOOD HURST & O'REARDON, LLP
TIMOTHY G. BLOOD (149343)
PAULA R. BROWN (254142)
JENNIFER L. MACPHERSON (202021)

By: *s/ Timothy G. Blood*
TIMOTHY G. BLOOD

501 West Broadway, Suite 1490
San Diego, CA 92101
Tel: 619/338-1100
619/338-1101 (fax)
tblood@bholaw.com
pbrown@bholaw.com
jmacpherson@bholaw.com

KAZEROUNI LAW GROUP, APC
ABBAS KAZEROUNIAN (249203)
MONA AMINI (296829)
245 Fischer Avenue, Unit D1
Costa Mesa, CA 92626
Tel: 800/400-6808
800/520-5523 (fax)
ak@kazlg.com

mona@kazlg.com

WOLF HALDENSTEIN ADLER
FREEMAN & HERZ LLP
RACHELE R. BYRD (190634)
750 B Street, Suite 1820
San Diego, CA 92101
Tel: 619/239-4599
619/234-4599 (fax)
byrd@whafh.com

CLAYEO C. ARNOLD, APC
M. ANDERSON BERRY (262879)
865 Howe Avenue
Sacramento, CA 95825
Tel: 916/777-7777
916/924-1829 (fax)
aberry@justice4you.com

MILBERG COLEMAN BRYSON
PHILLIPS GROSSMAN, PLLC
DAVID K. LIETZ (*PHV forthcoming*)
5335 Wisconsin Avenue NW, Suite 440
Washington, DC 20015-2052
dlietz@milberg.com

Attorneys for Plaintiffs Kolar and Miller and the Proposed Class

S|TRATEGE LAW, LLP
J. SCOTT SCHEPER (15547)
5060 N Harbor Drive, Suite 275
San Diego, CA 92106-2386
Tel: 619/677-5800
619/338-1101 (fax)
scheper@strategelaw.com

MARKOVITS, STOCK & DEMARCO, LLC
TERENCE R. COATES (Pro Hac Vice Forthcoming)
3825 Edwards Road, Suite 650
Cincinnati, OH 45209
Phone: (513) 651-3700
Fax: (513) 665-0219
tcoates@msdlegal.com

THE LYON FIRM, LLC
JOSEPH M. LYON (*PHV forthcoming*)
2754 Erie Avenue
Cincinnati, OH 45208
Phone: (513) 381-2333; Fax: (513) 721-1178
jlyon@thelyonfirm.com

Attorneys for Plaintiffs Maloney, Holmes, Moore, and Franklin and the Proposed Class

FEDERMAN & SHERWOOD
WILLIAM B. FEDERMAN (*PHV forthcoming*)
10205 N. Pennsylvania Ave.

Oklahoma City, OH 73120
Tel: 405/235-1560
wbf@federmanlaw.com
Attorneys for Plaintiff Brooke Roberts-Gooden

CERTIFICATE OF SERVICE

Ivo Kolar v. CSI Financial Services, LLC
San Diego Superior Court – Central Case No. 37-2021-00030426-CU-NP-CTL

Ronald Maloney v. Financial Services, LLC
San Diego Superior Court – Central Case No. 37-2021-00033113-CU-PO-CTL

I hereby certify that on April 22, 2022, I electronically filed the foregoing with the Clerk of the Court using One Legal Online Court Services, and electronically served the foregoing upon the attorney of record for each party in this case at the e-mail address(es) registered for such service through One Legal Online Court Services. Parties may access this filing through the Court's website.

I certify under penalty of perjury that the foregoing is true and correct. Executed on April 22, 2022.

s/ Janet Kohnenberger

Janet Kohnenberger
BLOOD HURST & O'REARDON, LLP
501 West Broadway, Suite 1490
San Diego, CA 92101
Tel: 619/338-1100
619/338-1101 (fax)
jkohnenberger@bholaw.com