Bibianne U. Fell (State Bar No. 234194)
FELL LAW, P.C.
l1956 Bernardo Plaza Dr. #53l,
San Diego, CA 92128
Telephone: (858) 201-3960
Email: bibi@fellfirm.com

William B. Federman*
wbf@federmanlaw.com
FEDERMAN & SHERWOOD
10205 N. Pennsylvania Ave.
Oklahoma City, OK 73120
Telephone: (405) 235-1560
Facsimile: (405) 239-2112

**Pro Hac Vice* application to be submitted

Counsel for Plaintiff and the Proposed Class

UNITED STATES DISTRICT COURT

SOUTHERN DISTRICT OF CALIFORNIA

BROOKE ROBERTS-GOODEN, individually and on behalf of all others similarly situated,

Plaintiff,
v.
CSI FINANCIAL SERVICES, LLC, d/b/a CLEARBALANCE HOLDINGS, LLC,

Defendant.

Case No.: **'21CV1352 BAS BGS**

CLASS ACTION COMPLAINT

JURY TRIAL DEMANDED

Plaintiff Brooke Roberts-Gooden ("Plaintiff"), individually and on behalf of all others similarly situated, and on behalf of the general public, for her Class Action Complaint, brings this action against defendant CSI Financial Services, LLC d/b/a ClearBalance Holdings, LLC (referred to herein as "ClearBalance," "Defendant," or the "Company") based on personal knowledge and the investigation of counsel, and alleges as follows:

I. INTRODUCTION

1. With this action, Plaintiff seeks to hold Defendant responsible for the harms it caused Plaintiff and the more than 200,000 similarly situated persons in the massive and preventable data breach of Defendant's inadequately protected email accounts.

2. Beginning on at least March 8, 2021, cyber criminals conducted a successful phishing campaign whereby they infiltrated Defendant's inadequately protected email accounts and gained access to confidential personal information and health information of the tens of thousands of individuals whose information was stored within these accounts ("Data Breach" or "Breach").[1] The Breach was not detected until nearly two months after the intrusion when the cyber criminals attempted to wire transfer funds from the impacted accounts. Following this discovery, Defendant launched an investigation into the Breach. The investigation revealed that multiple email accounts, and the data they contained, were accessed on several occasions between at least March 8, 2021 and April 26, 2021. Indeed, during the Breach, the cyber criminals succeeded in accessing the confidential personal information of nearly 210,000 individuals ("Breach Victims" or "Class members").[2]

---

[1] *See* https://apps.web.maine.gov/online/aeviewer/ME/40/10900d6e-0624-4c2f-a58a-6a1b6b798091.shtml (last accessed July 21, 2021).

[2] https://www.scmagazine.com/analysis/breach/phishing-attack-on-loan-provider-clearbalance-breaches-data-of-200k-patients (last accessed July 21, 2021).

3. The personal information taken by the cyber criminals includes: names, tax IDs, Social Security numbers, dates of birth, government-issued IDs, phone numbers, healthcare account numbers, balances, dates of service, loan numbers, personal banking information, clinical information, health insurance information, and full-face photographs (collectively, "Personal Information").[3]

4. ClearBalance is a leading provider of patient financing programs to U.S. hospitals and health systems. ClearBalance promotes itself as having one of the highest loan repayment rates in the industry. Defendant provides services in numerous states across the country, including California.

5. In order to receive financing services, Plaintiff and Class members were required to provide Defendant with their Personal Information and did so with the assurance and understanding that such information would be kept safe from unauthorized access. For example, Defendant's Privacy Policy assures its customers: "We use industry standard physical, technical and administrative security measures and safeguards to protect the confidentiality and security of your personal information."[4]

6. By taking possession and control of Plaintiff's and Class members' Personal Information, Defendant assumed a duty to securely store and protect the Personal Information of Plaintiff and the Class.

7. Defendant breached this duty and betrayed the trust of Plaintiff and Class members by failing to properly safeguard and protect their Personal Information, thus enabling cyber criminals to access, acquire, appropriate, compromise, disclose, encumber, exfiltrate, release, steal, misuse, and/or view it.

8. Defendant's misconduct – failing to timely implement adequate and reasonable measures to protect Plaintiff's and Class members' Personal

[3] https://healthitsecurity.com/news/clearbalancedata-incidentimpactsover-200000uspatientspii (last accessed July 21, 2021).
[4] https://www.myclearbalance.com/About/Privacy (last accessed July 21, 2021).

Information, failing to timely detect the Data Breach, failing to take adequate steps to prevent and stop the Data Breach, failing to disclose the material facts that it did not have adequate security practices in place to safeguard the Personal Information, failing to honor its promises and representations to protect Plaintiff's and Class members' Personal Information, and failing to provide timely and adequate notice of the Data Breach – caused substantial harm and injuries to Plaintiff and Class members across the United States.

9. Due to Defendant's negligence and failures, cyber criminals obtained and now possess everything they need to commit personal and medical identity theft and wreak havoc on the financial and personal lives of 209,719 individuals, for decades to come.

10. Plaintiff brings this class action lawsuit to hold Defendant responsible for its grossly negligent—indeed, reckless—failure to use statutorily required or reasonable industry cybersecurity measures to protect Class members' Personal Information.

11. Because Defendant presented such a soft target to cyber criminals, Plaintiff and Class members have already been subjected to violations of their privacy, fraud, and identity theft, or have been exposed to a heightened and imminent risk of certainly impending fraud and identity theft.

12. Thus, as a result of the Data Breach, Plaintiff and Class members have already suffered damages. For example, now that their Personal Information has been released into the criminal cyber domains, Plaintiff and Class members are at imminent and impending risk of identity theft. This risk will continue for the rest of their lives, as Plaintiff and Class members are now forced to deal with the danger of identity thieves possessing and using their Personal Information. In fact, Plaintiff Roberts-Gooden has already experienced identity theft in the form of fraudulent credit card charges and an account fraudulently opened in her name. Additionally, Plaintiff and Class members have already lost time and money

responding to and mitigating the impact of the Data Breach, which efforts are continuous and ongoing.

13. Plaintiff brings this action individually and on behalf of the Class and seeks actual damages, statutory damages, punitive damages, and restitution, with attorney fees, costs, and expenses, under California's Unfair Competition Law ("UCL"), Cal. Bus. Prof. Code § 17200, *et seq.*, and North Carolina's Deceptive Trade Practices Act, N.C. Gen. Stat. § 75-1.1, *et seq.*, and further sues Defendant for negligence (including negligence *per se*) and breach of contract, breach of the implied covenant of good faith and fair dealing, breach of confidence, and unjust enrichment. Plaintiff also seeks declaratory and injunctive relief, including significant improvements to Defendant's data security systems and protocols, future annual audits, Defendant-funded long-term credit monitoring services, and other remedies as the Court sees necessary and proper. incurred in bringing this action, and all other remedies this Court deems proper.

II. THE PARTIES

14. Plaintiff Brooke Roberts-Gooden is a citizen and resident of the City of Charlotte, North Carolina, in Mecklenburg County.

15. Defendant maintains its principal place of business in San Diego, California. Upon information and belief, Defendant is a citizen of California. As part of Defendant's business, Defendant collects substantial amounts of Personal Information. Upon information and belief, the information Defendant collects includes information that qualifies as "Personal information" under the California Consumer Privacy Act as well as other state data breach and information privacy acts and includes information that qualifies as "Medical information" under the federal Health Information Portability and Accountability Act ("HIPAA") and other state medical record protection acts.

III. JURISDICTION AND VENUE

16. Plaintiff incorporates by reference all allegations of the preceding paragraphs as though fully set forth herein.

17. This Court has diversity jurisdiction over this action under the Class Action Fairness Act (CAFA), 28 U.S.C. § 1332(d) because this is a class action involving more than 100 class members, the amount in controversy exceeds $5,000,000, exclusive of interest and costs, and Plaintiff and members of the Class are citizens of states that differ from Defendant.

18. This Court has personal jurisdiction over Defendant because Defendant conducts business in and have sufficient minimum contacts with California.

19. Venue is likewise proper as to Defendant in this District under 28 U.S.C. § 1391(a)(1) because Defendant's principal place of business is in this District and many of Defendant's acts complained of herein occurred within this District.

IV. FACTUAL ALLEGATIONS

A. The Notices Sent to Attorneys General

20. Beginning on at least March 8, 2021, third-party cyber criminals conducted a successful phishing campaign whereby they infiltrated Defendant's email accounts and gained access to confidential personal information and health information of the tens of thousands of individuals whose information was stored within these accounts. The Breach was not detected until nearly two months after the intrusion when the cyber criminals attempted to wire transfer funds from the impacted accounts. Ultimately, it was determined that multiple email accounts, and the data they contained, were accessed on several occasions between at least

March 8, 2021 and April 26, 2021 and that cyber criminals succeeded in accessing the Personal Information of nearly 210,000 individuals.[5]

21. In or around July 9, 2021, Defendant began filing with various state Attorneys General (including California) sample "Notice of Data Security Incident" letters that largely mirrored the language of the Notice sent to Plaintiff and Class members.

22. The sample "Notice of Data Security Incident" letter was filed with the Attorney General of California in accordance with California Civ. Code § 1798.82(f).

23. Pursuant to California Civ. Code § 1798.82(f), "[a] person or business that is required to issue a security breach notification pursuant to [§ 1798.82(a)] to more than 500 California residents as a result of a single breach of the security system shall electronically submit a single sample copy of that security breach notification, excluding any personally identifiable information, to the Attorney General."

24. Plaintiff's and Class members' Personal Information is "personal information" as defined by California Civ. Code § 1798.82(h).

25. Pursuant to California Civ. Code § 1798.82(a)(1), data breach notification letters are 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."

26. 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."

[5] https://www.scmagazine.com/analysis/breach/phishing-attack-on-loan-provider-clearbalance-breaches-data-of-200k-patients (last accessed July 21, 2021).

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

28. Thus, pursuant to California Civ. Code § 1798.82, Defendant reasonably believes that unencrypted personal information was acquired by an unauthorized person as a result of the Data Breach.

29. Further, pursuant to California Civ. Code § 1798.82, Defendant reasonably believes the security, confidentiality, or integrity of unencrypted personal information was compromised as a result of the Data Breach.

30. Based on these letters sent to numerous Attorneys General, including the Attorney General of California pursuant to California Civ. Code § 1798.82, it is reasonable for Plaintiff and Class members to believe that future harm (including identity theft) is real and imminent, and to take steps to mitigate that risk of future harm.

B. The Data Breach and Defendant's Belated Notice

31. It is apparent from the Notice sent to Plaintiff and the Class and from the sample "Notice of Data Security Incident" letters sent to state Attorneys General that the Personal Information contained within these email accounts was not encrypted.[6]

32. Following the phishing event, Defendant began working with a forensic firm to investigate the Breach. Based upon the investigation, the hackers were able to access multiple business email accounts between at least March 8, 2021 and April 26, 2021 where Plaintiff's and Class members' Personal Information was being held, unencrypted and unprotected.

33. Upon information and belief, the unauthorized third-party cyber criminal gained access to the Personal Information and has engaged in (and will

[6] https://oag.ca.gov/ecrime/databreach/reports/sb24-542757 (last accessed July 23, 2021).

continue to engage in) misuse of the Personal Information, including marketing and selling Plaintiff's and Class members' Personal Information on the dark web.

34. Despite learning of the Data Breach on April 26, 2021, it was not until July 9, 2021 that Defendant began notifying Class members that their Personal Information had been accessed by unauthorized cyber criminals.

35. Plaintiff and Class members were required to provide their Personal Information to Defendant with the reasonable expectation and mutual understanding that ClearBalance would comply with its obligations to keep such information confidential and secure from unauthorized access. Indeed, ClearBalance's website represents: "We respect the privacy of our customers and are committed to protecting their information…." and "…use industry standard physical, technical and administrative security measures and safeguards to protect the confidentiality and security of your personal information."[7]

36. Accordingly, Defendant had obligations created by reasonable industry standards, common law, statutory law, and its own assurances and representations to its patient customers to keep their Personal Information confidential and to protect such Personal Information from unauthorized access.

37. Nevertheless, Defendant failed to spend sufficient resources on preventing external access, detecting outside infiltration, and training its employees to identify email-borne threats and defend against them.

38. The stolen Personal Information at issue has great value to the hackers, due to the large number of individuals affected and the fact that health insurance information and Social Security numbers were part of the data that was compromised.

[7] https://www.myclearbalance.com/About/Privacy (last accessed July 23, 2021).

C. Plaintiff's Experience

39. Plaintiff received a letter from Defendant dated July 9, 2021 informing her that her personal information, including her Social Security number, date of birth, loan number, loan balance, date of birth, and telephone number were compromised in the Data Breach.[8]

40. Plaintiff is a customer of ClearBalance. To receive services from Defendant, Plaintiff was required to provide her Personal Information to ClearBalance.

41. Because of the Data Breach, Plaintiff's Personal Information is now in the hands of cyber criminals. In addition to the identity theft and fraud she has already experienced as of the date of this Complaint, Plaintiff and all Class members are now imminently at risk of crippling future identity theft and fraud.

42. To the best of her knowledge, Plaintiff has never before been a victim of a data breach.

43. Immediately following the Data Breach, Plaintiff began receiving notifications of attempts to open credit cards in her name. Plaintiff also recently learned that someone has fraudulently opened a bank account in her name. Plaintiff believes these acts of fraud and identity theft were caused by the Data Breach.

44. These experiences have been distressing to Plaintiff and have caused her anxiety. Plaintiff has already spent time investigating and responding to the Data Breach, including closing the bank account that was fraudulently opened in her name.

[8] The letter Plaintiff received was substantially similar to the breach notification letter Defendant provided to California's Attorney General: https://oag.ca.gov/ecrime/databreach/reports/sb24-542757 (last accessed July 23, 2021).

45. Because the Data Breach was an intentional hack by cyber criminals seeking information of value that they could exploit, Plaintiff is at imminent risk of severe identity theft and exploitation.

46. Plaintiff has also suffered injury directly and proximately caused by the Data Breach, including: (a) theft of Plaintiff's valuable Personal Information; (b) the imminent and certain impending injury flowing from fraud and identity theft posed by Plaintiff's Personal Information being placed in the hands of cyber criminals; (c) damages to and diminution in value of Plaintiff's Personal Information that was entrusted to Defendant for the sole purpose of obtaining services relating to the payment of Plaintiff's medical bills with the understanding that Defendant would safeguard this information against disclosure; (d) loss of the benefit of the bargain with Defendant to provide adequate and reasonable data security—*i.e.*, the difference in value between what Plaintiff should have received from Defendant and Defendant's defective and deficient performance of that obligation by failing to provide reasonable and adequate data security and failing to protect Plaintiff's Personal Information; and (e) continued risk to Plaintiff's Personal Information, which remains in the possession of Defendant and which is subject to further breaches so long as Defendant fails to undertake appropriate and adequate measures to protect the Personal Information that was entrusted to Defendant.

D. Defendant had an Obligation to Protect Personal Information under the Law and the Applicable Standard of Care

47. Upon information and belief, Defendant is covered by HIPAA (45 C.F.R. § 160.102). As such, it is required to comply with the HIPAA Privacy Rule and Security Rule, 45 C.F.R. Part 160 and Part 164, Subparts A and E ("Standards for Privacy of Individually Identifiable Health Information"), and Security Rule ("Security Standards for the Protection of Electronic Protected Health Information"), 45 C.F.R. Part 160 and Part 164, Subparts A and C.

48. HIPAA's Privacy Rule or *Security Standards for the Protection of Electronic Protected Health Information* establishes a national set of security standards for protecting health information, including health information that is kept or transferred in electronic form.

49. HIPAA requires Defendant to "comply with the applicable standards, implementation specifications, and requirements" of HIPAA "with respect to electronic protected health information." 45 C.F.R. § 164.302.

50. "Electronic protected health information" is "individually identifiable health information … that is (i) transmitted by electronic media; maintained in electronic media." 45 C.F.R. § 160.103.

51. HIPAA's Security Rule requires Defendant to do the following:

a. Ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity or business associate creates, receives, maintains, or transmits;

b. Protect against any reasonably anticipated threats or hazards to the security or integrity of such information;

c. Protect against any reasonably anticipated uses or disclosures of such information that are not permitted; and

d. Ensure compliance by their workforce.

52. HIPAA also requires Defendant to "review and modify the security measures implemented … as needed to continue provision of reasonable and appropriate protection of electronic protected health information." 45 C.F.R. § 164.306(e).

53. Additionally, HIPAA requires Defendant to "[i]mplement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights." 45 C.F.R. § 164.312(a)(1).

54. The HIPAA Breach Notification Rule, 45 C.F.R. §§ 164.400-414, further requires Defendant to provide notice of the Data Breach to each affected individual "without unreasonable delay and in no case later than 60 days following discovery of the breach." Cal. Civ. Code §1798.82 similarly requires breach notification to "be made in the most expedient time possible and without unreasonable delay."

55. 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).

56. Defendant is further required by various states' laws and regulations to protect Plaintiff's and Class members' Personal Information.

57. For example, the California Consumer Privacy Act (Cal. Civ. Code § 1798.100, *et seq*.) ("CCPA") requires Defendant to take reasonable steps and employ reasonable methods of safeguarding personal information it collects and maintains, including the Personal Information that Defendant failed to protect and allowed to be exposed in its Data Breach. *See* Cal. Civ. Code §1798.81.5.

58. Under the CCPA, the breach of unencrypted personal information is direct evidence that Defendant violated its duty to provide reasonable security procedures and practices to protect the sensitive information. *See* Cal. Civ. Code §1798.150(a)(1).

59. Moreover, Defendant represented to Plaintiff and Class members that it took appropriate steps to reasonably protect its customers' Personal Information. For example, ClearBalance's website represents: "We respect the privacy of our customers and are committed to protecting their information…." and "… use

industry standard physical, technical and administrative security measures and safeguards to protect the confidentiality and security of your personal information."[9] Defendant's website further includes a California Privacy Notice purporting to comply with the CCPA.[10]

60. In addition to its obligations under federal and state laws, Defendant owed a duty to Plaintiff and Class members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the Personal Information in their possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons. Defendant owed a duty to Plaintiff 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 the Personal Information of the Class.

61. Defendant owed a duty to Plaintiff and the Class to design, maintain, and test its computer and email systems to ensure that the Personal Information in its possession was adequately secured and protected.

62. Defendant owed a duty to Plaintiff and the Class to create and implement reasonable data security practices and procedures to protect the Personal Information in its possession, including adequately training its employees (and others who accessed Personal Information within its computer systems) on how to adequately protect Personal Information.

63. Defendant owed a duty to Plaintiff and the Class to implement processes that would detect a breach on its data security systems in a timely manner.

64. Defendant owed a duty to Plaintiff and the Class to act upon data security warnings and alerts in a timely fashion.

---

[9] https://www.myclearbalance.com/About/Privacy (last accessed July 23, 2021).

[10] https://www.myclearbalance.com/About/CAPrivacy (last accessed July 23, 2021).

65. Defendant owed a duty to Plaintiff and the Class to adequately train and supervise its employees to identify and avoid any phishing emails that make it past its email filtering service.

66. Defendant owed a duty to Plaintiff and the Class to disclose if its computer systems and data security practices were inadequate to safeguard individuals' Personal Information from theft because such an inadequacy would be a material fact in the decision to entrust Personal Information with Defendant.

67. Defendant owed a duty to Plaintiff and the Class to disclose in a timely and accurate manner when data breaches occurred.

68. Defendant owed a duty of care to Plaintiff and the Class because they were foreseeable and probable victims of any inadequate data security practices.

E. Defendant was on Notice of Cyber Attack Threats and of the Inadequacy of their Data Security

69. Defendant was on notice that companies, including companies operating within and aiding the healthcare industry have been targets for cyberattacks.

70. Defendant was on notice that the FBI has recently been concerned about data security in the healthcare industry. In August 2014, after a cyberattack on Community Health Systems, Inc., the FBI warned companies within the healthcare industry that hackers were targeting them. The warning stated that "[t]he FBI has observed malicious actors targeting healthcare related systems, perhaps for the purpose of obtaining the Protected Healthcare Information (PHI) and/or Personally Identifiable Information (PII)."[11]

71. The American Medical Association ("AMA") has also warned companies about the importance of protecting patients' confidential information:

> Cybersecurity is not just a technical issue; it's a patient safety issue. AMA research has revealed that 83% of physicians work in a

[11] Jim Finkle, *FBI Warns Healthcare Firms that they are Targeted by Hackers*, REUTERS (Aug. 2014), http://www.reuters.com/article/2014/08/20/us-cybersecurity-healthcare-fbi-idUSKBN0GK24U20140820.

> practice that has experienced some kind of cyberattack. Unfortunately, practices are learning that cyberattacks not only threaten the privacy and security of patients' health and financial information, but also patient access to care.[12]

72. Defendant was also on notice of the importance of data encryption of Personal Information. Defendant knew it kept Personal Information in its email accounts and yet it appears Defendant did not encrypt these email accounts or the information contented within them.

73. The United States Department of Health and Human Services' Office for Civil Rights urges the use of encryption of data containing sensitive personal information. As long ago as 2014, the Department fined two healthcare companies approximately two million dollars for failing to encrypt laptops containing sensitive personal information. In announcing the fines, Susan McAndrew, the DHHS's Office of Human Rights' deputy director of health information privacy, stated "[o]ur message to these organizations is simple: encryption is your best defense against these incidents."[13]

74. As a company operating within the healthcare sector, and a covered entity or business associate under HIPAA, Defendant should have known about its weakness toward email-related threats and sought better protection for the Personal Information accumulating in its business email accounts.

75. For companies that provide services within the healthcare industry, the number one threat vector from a cyber security standpoint is phishing. Cybersecurity firm Proofpoint reports that "phishing is the initial point of compromise in most significant [healthcare] security incidents, according to a

[12] Andis Robeznieks, *Cybersecurity: Ransomware attacks shut down clinics, hospitals*, AM. MED. ASS'N (Oct. 4, 2019), https://www.ama-assn.org/practice-management/sustainability/cybersecurity-ransomeware-attacks-shut-down-clinics-hospitals.

[13] "Stolen Laptops Lead to Important HIPAA Settlements," U.S. Dep't of Health and Human Services (Apr. 22, 2014), available at https://wayback.archive-it.org/3926/20170127085330/https://www.hhs.gov/about/news/2014/04/22/stolen-laptops-lead-to-important-hipaa-settlements.html.

recent report from the Healthcare Information and Management Systems Society (HIMSS). And yet, 18% of healthcare organizations fail to conduct phishing tests, a finding HIMSS describes as 'incredible.'"[14]

76. The report from Proofpoint was published March 27, 2019, and summarized findings of recent healthcare industry cyber threat surveys and recounted good, common sense steps that the companies should follow to prevent email-related cyberattacks.

77. One of the best protections against email related threats is security awareness training and testing on a regular basis. This should be a key part of a company's ongoing training of its employees. "[S]ince phishing is still a significant, initial point of compromise, additional work needs to be done to further lower the click rate," the HIMSS report states. "This can be done through more frequent security awareness training, phishing simulation, and better monitoring of metrics pertaining to phishing (including whether there are any particular repeat offenders)."[15]

78. Similarly, ProtonMail Technologies publishes a guide for IT Security to small businesses. In its 2019 guide, ProtonMail dedicates a full chapter of its e-book guide to the danger of phishing and ways to prevent a small business from falling prey to it. It reports:

> Phishing and fraud are becoming ever more extensive problems. A recent threat survey from the cybersecurity firm Proofpoint stated that between 2017 and 2018, email-based attacks on businesses increased 476 percent. The FBI reported that these types of attacks cost companies around the world $12 billion annually.
>
> Similar to your overall IT security, your email security relies on training your employees to implement security best practices and to recognize possible phishing attempts. This must be deeply ingrained into every staff member so that

[14] Aaron Jensen, *Healthcare Phishing Statistics: 2019 HIMSS Survey Results* (Mar. 27, 2019), https://www.proofpoint.com/us/security-awareness/post/healthcare-phishing-statistics-2019-himss-survey-results.
[15] *Id.*

every time they check their emails, they are alert to the possibility of malicious action.[16]

79. The guidance that ProtonMail provides non-healthcare industry small businesses is likely still not adequate for a company like ClearBalance, with the heightened healthcare standard of care based on HIPAA and the increased danger from the sensitivity and wealth of personal information and health-related information it retains. However, ProtonMail's guidance is informative for showing how inadequately Defendant protected the Personal Information of Plaintiff and the Class. ProofPoint lists numerous tools under the heading, "How to Prevent Phishing":

a. **Training:** "Training your employees on how to recognize phishing emails and what to do when they encounter one is the first and most important step in maintaining email security. *This training should be continuous as well. . . .*"

b. **Limit Public Information:** "Attackers cannot target your employees if they don't know their email addresses. Don't publish non-essential contact details on your website or any public directories . . . ."

c. **Carefully check emails:** "First off, your employees should be skeptical anytime they receive an email from an unknown sender. Second, most phishing emails are riddled with typos, odd syntax, or stilted language. Finally, check the 'From' address to see if it is odd . . . . If an email looks suspicious, employees should report it."

[16] *The ProtonMail Guide to IT Security for Small Businesses*, PROTONMAIL (2019), available at https://protonmail.com/it-security-complete-guide-for-businesses.

d. **Beware of links and attachments:** "Do not click on links or download attachments without verifying the source first and establishing the legitimacy of the link or attachment…"

e. **Do not automatically download remote content:** "Remote content in emails, like photos, can run scripts on your computer that you are not expecting, and advanced hackers can hide malicious code in them. You should configure your email service provider to not automatically download remote content. This will allow you to verify an email is legitimate before you run any unknown scripts contained in it."

f. **Hover over hyperlinks:** "Never click on hyperlinked text without hovering your cursor over the link first to check the destination URL, which should appear in the lower corner of your window. Sometimes the hacker might disguise a malicious link as a short URL." [Proofpoint notes that there are tools online available for retrieving original URLs from shortened ones.]

g. **If in doubt, investigate:** "Often phishing emails will try to create a false sense of urgency by saying something requires your immediate action. However, if your employees are not sure if an email is genuine, they should not be afraid to take extra time to verify the email. This might include asking a colleague, your IT security lead, looking up the website of the

service the email is purportedly from, or, if they have a phone number, calling the institution, colleague, or client that sent the email."

h. **Take preventative measures:** "Using an end-to-end encrypted email service gives your business's emails an added layer of protection in the case of a data breach. A spam filter will remove the numerous random emails that you might receive, making it more difficult for a phishing attack to get through. Finally, other tools, like Domain-based Message Authentication, Reporting, and Conformance (DMARC) help you be sure that the email came from the person it claims to come from, making it easier to identify potential phishing attacks."[17]

80. As mentioned, these are basic, common-sense email security measures that every business, whether in healthcare or not, should be doing. By adequately taking these common-sense solutions, Defendant could have prevented this Data Breach from occurring.

F. Cyber Criminals Will Use Plaintiff's and Class Members' Personal Information to Defraud Them

81. Plaintiff and Class members' Personal Information is of great value to hackers and cyber criminals, and the data stolen in the Data Breach has been used and will continue to be used in a variety of sordid ways for criminals to exploit Plaintiff and the Class members and to profit off their misfortune.

[17] *Id.*

82. Each year, identity theft causes tens of billions of dollars of losses to victims in the United States.[18] For example, with the Personal Information stolen in the Data Breach, including Social Security numbers, identity thieves can open financial accounts, apply for credit, file fraudulent tax returns, commit crimes, create false driver's licenses and other forms of identification and sell them to other criminals or undocumented immigrants, steal government benefits, give breach victims' names to police during arrests, and many other harmful forms of identity theft.[19] These criminal activities have and will result in devastating financial and personal losses to Plaintiff and Class members.

83. Personal Information is such a valuable commodity to identity thieves that once it has been compromised, criminals will use it and trade the information on the cyber black-market for years.[20]

84. For example, it is believed that certain Personal Information compromised in the 2017 Experian data breach was being used, three years later, by identity thieves to apply for COVID-19-related benefits in the state of Oklahoma.[21]

85. This was a financially motivated Data Breach, as apparent from the discovery of the cyber criminals seeking to profit off the sale of Plaintiff's and the Class members' Personal Information on the dark web. The Personal Information

---

[18] "Facts + Statistics: Identity Theft and Cybercrime," Insurance Info. Inst., https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime (discussing Javelin Strategy & Research's report "2018 Identity Fraud: Fraud Enters a New Era of Complexity").

[19] *See, e.g.*, Christine DiGangi, *5 Ways an Identity Thief Can Use Your Social Security Number*, Nov. 2, 2017, https://blog.credit.com/2017/11/5-things-an-identity-thief-can-do-with-your-social-security-number-108597/.

[20] *Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown*, GAO, July 5, 2007, https://www.gao.gov/assets/270/262904.htmlu

[21] *See https://www.engadget.com/stolen-data-used-for-unemployment-fraud-ring-174618050.html; see also* https://www.wired.com/story/nigerian-scammers-unemployment-system-scattered-canary/.

exposed in this Data Breach are valuable to identity thieves for use in the kinds of criminal activity described herein.

86. These risks are both certainly impending and substantial. As the FTC has reported, if hackers get access to personally identifiable information, they will use it.[22]

87. Hackers may not use the accessed information right away. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches:

> [I]n 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.[23]

88. Medical-related identity theft is one of the most common, most expensive, and most difficult to prevent forms of identity theft. According to Kaiser Health News, "medical-related identity theft accounted for 43 percent of all identity thefts reported in the United States in 2013…," which is more than identity thefts involving banking and finance, the government and the military, or education.[24]

89. As indicated by James Trainor, second in command at the FBI's cyber security division: "Medical records are a gold mine for criminals—they can access a patient's name, DOB, Social Security and insurance numbers, and even

[22] Ari Lazarus, *How fast will identity thieves use stolen info?*, FED. TRADE COMM'N (May 24, 2017), https://www.consumer.ftc.gov/blog/2017/05/how-fast-will-identity-thieves-use-stolen-info.

[23] *Data Breaches Are Frequent*, *supra* note 11.

[24] Michael Ollove, "The Rise of Medical Identity Theft in Healthcare," Kaiser Health News, Feb. 7, 2014, https://khn.org/news/rise-of-indentity-theft/.

financial information all in one place."[25] A complete identity theft kit that includes health insurance credentials may be worth up to $1,000 on the black market.[26]

90. If cyber criminals manage to steal 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 has exposed the Plaintiff and Class members.

91. As described above, identity theft victims must spend countless hours and large amounts of money repairing the impact to their credit.[27]

92. With this Data Breach, identity thieves have already started to prey on the victims, and one can reasonably anticipate this will continue.

93. Victims of the Data Breach, like Plaintiff and other Class members, must spend many hours and large amounts of money protecting themselves from the current and future negative impacts to their credit because of the Data Breach.[28]

94. In fact, as a direct and proximate result of the Data Breach, Plaintiff and the Class have suffered, and have been placed at an imminent, immediate, and continuing increased risk of suffering, harm from fraud and identity theft. Plaintiff and the Class must now take the time and effort and spend the money to mitigate the actual and potential impact of the Data Breach on their everyday lives, including purchasing identity theft and credit monitoring services, placing

---

[25] IDExperts, *You Got It, They Want It: Criminals Targeting Your Private Healthcare Data, New Ponemon Study Shows*, https://www.idexpertscorp.com/knowedge-center/single/you-got-it-they-want-it-criminals-are-targeting-your-private-healthcare-dat.

[26] *Managing cyber risks in an interconnected world*, PRICEWATERHOUSECOOPERS: Key findings from The Global State of Information Security Survey 2015, https://www.pwc.com/gx/en/consulting-services/information-security-survey/assets/the-global-state-of-information-security-survey-2015.pdf.

[27] "Guide for Assisting Identity Theft Victims," Federal Trade Commission, 4 (Sept. 2013), http://www.consumer.ftc.gov/articles/pdf-0119-guide-assisting-id-theft-victims.pdf.

[28] "Guide for Assisting Identity Theft Victims," Federal Trade Commission, 4 (Sept. 2013), http://www.consumer.ftc.gov/articles/pdf-0119-guide-assisting-id-theft-victims.pdf.

"freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, healthcare providers, closing or modifying financial accounts, and closely reviewing and monitoring bank accounts, credit reports, and health insurance account information for unauthorized activity for years to come.

95. Plaintiff and the Class have suffered, and continue to suffer, actual harms for which they are entitled to compensation, including:

a. Trespass, damage to, and theft of their personal property including Personal Information;

b. Improper disclosure of their Personal Information;

c. The imminent and certainly impending injury flowing from potential fraud and identity theft posed by their Personal Information being placed in the hands of criminals and having been already misused;

d. The imminent and certainly impending risk of having their Personal Information used against them by spam callers to defraud them;

e. Damages flowing from Defendant's untimely and inadequate notification of the data breach;

f. Loss of privacy suffered as a result of the Data Breach;

g. Ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably expended to remedy or mitigate the effects of the data breach;

h. Ascertainable losses in the form of deprivation of the value of patients' personal information for which there is a well-established and quantifiable national and international market;

i. The loss of use of and access to their credit, accounts, and/or funds;

j. Damage to their credit due to fraudulent use of their Personal Information; and

k. Increased cost of borrowing, insurance, deposits and other items which are adversely affected by a reduced credit score.

96. Moreover, Plaintiff and Class members have an interest in ensuring that their information, which remains in the possession of Defendant, is protected from further breaches by the implementation of industry standard and statutorily compliant security measures and safeguards. Defendant has shown itself to be incapable of protecting Plaintiff's and Class members' Personal Information.

97. Plaintiff and Class members are desperately trying to mitigate the damage that Defendant has caused them but, given the Personal Information Defendant made accessible to hackers, they are certain to incur additional damages. Because identity thieves have their Personal Information, Plaintiff and all Class members will need to have identity theft monitoring protection for the rest of their lives. Some may even need to go through the long and arduous process of getting a new Social Security number, with all the loss of credit and employment difficulties that come with this change.[29]

98. None of this should have happened. The Data Breach was preventable.

G. Defendant Could Have Prevented the Data Breach but Failed to Adequately Protect Plaintiff's and Class Members' Personal Information

99. Data breaches are preventable.[30] 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

[29] *Will a New Social Security Number Affect Your Credit?*, LEXINGTON LAW (Nov. 16, 2015), https://www.lexingtonlaw.com/blog/credit-101/will-a-new-social-security-number-affect-your-credit.html.

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

correct design and implementation of appropriate security solutions."[31] 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 . . . ."[32]

100. "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*."[33]

101. Defendant required Plaintiff and Class members to surrender their Personal Information – including but not limited to their names, addresses, Social Security numbers, medical information, and health insurance information – and was entrusted with properly holding, safeguarding, and protecting against unlawful disclosure of such Personal Information.

102. Many failures laid the groundwork for the success ("success" from a cybercriminal's viewpoint) of the Data Breach, starting with Defendant's failure to incur the costs necessary to implement adequate and reasonable cyber security procedures and protocols necessary to protect Plaintiff's and Class members' Personal Information.

103. Defendant maintained the Personal Information in a reckless manner. In particular, the Personal Information was maintained and/or exchanged, unencrypted, in Defendant's business email accounts that were maintained in a condition vulnerable to cyberattacks.

104. Defendant knew, or reasonably should have known, of the importance of safeguarding Personal Information and of the foreseeable consequences that would occur if Plaintiff's and Class members' Personal

---

[31] *Id.* at 17.
[32] *Id.* at 28.
[33] *Id.*

Information was stolen, including the significant costs that would be placed on Plaintiff and Class members as a result of a breach.

105. The mechanism of the cyberattack and potential for improper disclosure of Plaintiff's and Class members' Personal Information was a known risk to Defendant, and thus Defendant was on notice that failing to take necessary steps to secure Plaintiff's and Class members' Personal Information from those risks left that information in a dangerous condition.

106. Defendant disregarded the rights of Plaintiff and Class members by, *inter alia*, (i) intentionally, willfully, recklessly, or negligently failing to take adequate and reasonable measures to ensure that its business email accounts 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 Plaintiff's and Class members' Personal 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 Plaintiff and Class members prompt and accurate notice of the Data Breach.

V. CLASS ACTION ALLEGATIONS

107. The State of California has a significant interest in regulating the conduct of businesses operating within its borders. California seeks to protect the rights and interests of citizens of the United States against a company headquartered and doing business in California. California has a greater interest in the nationwide claims of Plaintiff and members of the Nationwide Class (defined below) than any other state, and is most intimately concerned with the claims and outcome of this litigation.

108. The corporate headquarters of ClearBalance, located in San Diego, California, is the "nerve center" of its business activities – the place where its high-level officers direct, control, and coordinate the company's activities,

including its data security functions and major policy, financial, and legal decisions.

109. Defendant's response to the Data Breach at issue here, and the corporate decisions surrounding such response, were made from and in California.

110. Defendant's breaches of duty to Plaintiff and Class members emanated from California.

111. Application of California law to the Nationwide Class with respect to Plaintiff's and Class members' claims is neither arbitrary nor fundamentally unfair because California has significant contacts and a significant aggregation of contacts that create a state interest in the claims of Plaintiff and the Nationwide Class.

112. Under California's choice of law principles, which are applicable to this action, the common law of California applies to the nationwide common law claims of all Nationwide Class members. Additionally, given California's significant interest in regulating the conduct of businesses operating within its borders, California's Unfair Competition Law may be applied to non-resident consumer plaintiffs as against this resident-defendant. Further, the corporate headquarters of ClearBalance are located in San Diego, California, which is the "nerve center" of Defendant's business activities – the place where its high-level officers direct, control, and coordinate the company's activities, including its data security functions and major policy, financial, and legal decisions.

VI. CLASS ACTION ALLEGATIONS

113. Plaintiff incorporates by reference all allegations of the preceding paragraphs as though fully set forth herein.

114. Plaintiff brings all claims as class claims under Federal Rule of Civil Procedure 23. Plaintiff asserts all claims on behalf of the Nationwide Class, defined as follows:

> All persons residing in the United States whose personal information was compromised as a result of the ClearBalance Data Breach that occurred in March and April 2021.

115. Plaintiff also proposes the following Subclass, as follows:

> North Carolina Subclass: All residents of North Carolina whose personal information was compromised as a result of the ClearBalance Data Breach that occurred in March and April 2021.

116. Also, in the alternative, Plaintiff requests additional subclasses as necessary based on the types of Personal Information that were compromised.

117. Plaintiff reserves the right to amend the above definitions or to propose alternative or additional subclasses in subsequent pleadings and motions for class certification.

118. The proposed Nationwide Class and Subclass (collectively referred to herein as the "Class" unless otherwise specified) meet the requirements of Fed. R. Civ. P. 23(a), (b)(1), (b)(2), (b)(3), and (c)(4).

119. **Numerosity:** The proposed Class is believed to be so numerous that joinder of all members is impracticable. The proposed Subclass is also believed to be so numerous that joinder of all members would be impractical.

120. **Typicality:** Plaintiff's claims are typical of the claims of the Class. Plaintiff and all members of the Class were injured through Defendant's uniform misconduct. The same event and conduct that gave rise to Plaintiff's claims are identical to those that give rise to the claims of every other Class member because Plaintiff and each member of the Class had their sensitive Personal Information compromised in the same way by the same conduct of Defendant.

121. **Adequacy:** Plaintiff is an adequate representative of the Class because her interests do not conflict with the interests of the Class and proposed Subclass that she seeks to represent; Plaintiff has retained counsel competent and highly experienced in data breach class action litigation; and Plaintiff and

Plaintiff's counsel intend to prosecute this action vigorously. The interests of the Class will be fairly and adequately protected by Plaintiff and her counsel.

122. **Superiority:** A class action is superior to other available means of fair and efficient adjudication of the claims of Plaintiff and the Class. The injury suffered by each individual Class member is relatively small in comparison to the burden and expense of individual prosecution of complex and expensive litigation. It would be very difficult, if not impossible, for members of the Class individually to effectively redress Defendant's wrongdoing. Even if Class members could afford such individual litigation, the court system could not. Individualized litigation presents a potential for inconsistent or contradictory judgments. Individualized litigation increases the delay and expense to all parties, and to the court system, presented by the complex legal and factual issues of the case. By contrast, the class action device presents far fewer management difficulties and provides benefits of single adjudication, economy of scale, and comprehensive supervision by a single court.

123. **Commonality and Predominance:** There are many questions of law and fact common to the claims of Plaintiff and the other members of the Class, and those questions predominate over any questions that may affect individual members of the Class. Common questions for the Class include:

a. Whether Defendant engaged in the wrongful conduct alleged herein;

b. Whether Defendant failed to adequately safeguard Plaintiff's and the Class's Personal Information;

c. Whether Defendant's email and computer systems and data security practices used to protect Plaintiff's and Class members' Personal Information violated the FTC Act, HIPAA, and/or state laws and/or Defendant's other duties discussed herein;

d. Whether Defendant owed a duty to Plaintiff and the Class to adequately protect their Personal Information, and whether it breached this duty;

e. Whether Defendant knew or should have known that its computer and network security systems and business email accounts were vulnerable to a data breach;

f. Whether Defendant's conduct, including its failure to act, resulted in or was the proximate cause of the Data Breach;

g. Whether Defendant breached contractual duties owed to Plaintiff and the Class to use reasonable care in protecting their Personal Information;

h. Whether Defendant failed to adequately respond to the Data Breach, including failing to investigate it diligently and notify affected individuals in the most expedient time possible and without unreasonable delay, and whether this caused damages to Plaintiff and the Class;

i. Whether Defendant continues to breach duties to Plaintiff and the Class;

j. Whether Plaintiff and the Class suffered injury as a proximate result of Defendant's negligent actions or failures to act;

k. Whether Plaintiff and the Class are entitled to recover damages, equitable relief, and other relief;

l. Whether injunctive relief is appropriate and, if so, what injunctive relief is necessary to redress the imminent and currently ongoing harm faced by Plaintiff and members of the Class and the general public;

m. Whether Defendant's actions alleged herein constitute gross negligence; and

n. Whether Plaintiff and Class members are entitled to punitive damages.

VII. CAUSES OF ACTION

A. COUNT I – NEGLIGENCE

124. Plaintiff incorporates by reference all allegations of the preceding paragraphs as though fully set forth herein.

125. Defendant solicited, gathered, and stored the Personal Information of Plaintiff and the Class as part of the operation of its business.

126. Upon accepting and storing the Personal Information of Plaintiff and Class members, Defendant undertook and owed a duty to Plaintiff and Class members to exercise reasonable care to secure and safeguard that information and to use secure methods to do so.

127. Defendant had full knowledge of the sensitivity of the Personal Information, the types of harm that Plaintiff and Class members could and would suffer if the Personal Information was wrongfully disclosed, and the importance of adequate security.

128. Plaintiff and Class members were the foreseeable victims of any inadequate safety and security practices on the part of Defendant. Plaintiff and the Class members had no ability to protect their Personal Information that was in Defendant's possession. As such, a special relationship existed between Defendant and Plaintiff and the Class.

129. Defendant was well aware of the fact that cyber criminals routinely target large corporations through cyberattacks in an attempt to steal sensitive personal and medical information.

130. Defendant owed Plaintiff and the Class members a common law duty to use reasonable care to avoid causing foreseeable risk of harm to Plaintiff and the Class when obtaining, storing, using, and managing personal information, including taking action to reasonably safeguard such data and providing

notification to Plaintiff and the Class members of any breach in a timely manner so that appropriate action could be taken to minimize losses.

131. Defendant's duty extended to protecting Plaintiff and the Class from the risk of foreseeable criminal conduct of third parties, which has been recognized in situations where the actor's own conduct or misconduct exposes another to the risk or defeats protections put in place to guard against the risk, or where the parties are in a special relationship. *See* Restatement (Second) of Torts § 302B. Numerous courts and legislatures also have recognized the existence of a specific duty to reasonably safeguard personal information.

132. Defendant had duties to protect and safeguard the Personal Information of Plaintiff and the Class from being vulnerable to cyberattacks by taking common-sense precautions when dealing with sensitive Personal Information. Additional duties that Defendant owed Plaintiff and the Class include:

a. To exercise reasonable care in designing, implementing, maintaining, monitoring, and testing Defendant's networks, systems, email accounts, protocols, policies, procedures and practices to ensure that Plaintiff's and Class members' Personal Information was adequately secured from impermissible release, disclosure, and publication;

b. To protect Plaintiff's and Class members' Personal Information in its possession by using reasonable and adequate security procedures and systems;

c. To implement processes to quickly detect a data breach, security incident, or intrusion involving its business email system, networks and servers; and

d. To promptly notify Plaintiff and Class members of any data breach, security incident, or intrusion that affected or may have affected their Personal Information.

133. Only Defendant was in a position to ensure that its systems and protocols were sufficient to protect the Personal Information that Plaintiff and the Class had entrusted to it.

134. Defendant breached its duty of care by failing to adequately protect Plaintiff's and Class members' Personal Information. Defendant breached its duties by, among other things:

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

b. Failing to protect the Personal Information in its possession by using reasonable and adequate security procedures and systems;

c. Failing to adequately and properly audit, test, and train its employees to avoid phishing emails;

d. Failing to use adequate email security systems, including healthcare industry standard SPAM filters, DMARC enforcement, and/or Sender Policy Framework enforcement to protect against phishing emails;

e. Failing to adequately and properly audit, test, and train its employees regarding how to properly and securely transmit and store Personal Information;

f. Failing to adequately train its employees to not store Personal Information in their email inboxes longer than absolutely necessary for the specific purpose that it was sent or received;

g. Failing to consistently enforce security policies aimed at protecting Plaintiff's and the Class's Personal Information;

h. Failing to implement processes to quickly detect data breaches, security incidents, or intrusions;

i. Failing to promptly notify Plaintiff and Class members of the Data Breach that affected their Personal Information.

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

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

137. Through Defendant's acts and omissions described herein, including but not limited to Defendant's failure to protect the Personal Information of Plaintiff and Class members from being stolen and misused, Defendant unlawfully breached its duty to use reasonable care to adequately protect and secure the Personal Information of Plaintiff and Class members while it was within Defendant's possession and control.

138. Further, through its failure to provide timely and clear notification of the Data Breach to Plaintiff and Class members, Defendant prevented Plaintiff and Class members from taking meaningful, proactive steps toward securing their Personal Information and mitigating damages.

139. As a result of the Data Breach, Plaintiff and Class members have spent time, effort, and money to mitigate the actual and potential impact of the Data Breach on their lives, including but not limited to, responding to fraudulent activity, closely monitoring bank account activity, and examining credit reports and statements sent from providers and their insurance companies.

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

141. The damages Plaintiff and the Class have suffered (as alleged above) and will suffer were and are the direct and proximate result of Defendant's grossly negligent conduct.

142. In addition to its duties under common law, Defendant had additional duties imposed by statute and regulations, including the duties under HIPAA, the FTC Act, and the CCPA. The harms which occurred as a result of Defendant's failure to observe these duties, including the loss of privacy, lost time and expense, and significant risk of identity theft are the types of harm that these statutes and regulations intended to prevent.

143. Defendant violated these statutes when it engaged in the actions and omissions alleged herein, and Plaintiff's and Class members' injuries were a direct and proximate result of Defendant's violations of these statutes. Plaintiff therefore is entitled to the evidentiary presumptions for negligence *per se* under Cal. Evid. Code § 669.

144. Pursuant to the FTC Act, 15 U.S.C. § 45(a), Defendant owed a duty to Plaintiff and the Class to provide fair and adequate computer systems and data security to safeguard the Personal Information of Plaintiff and the Class.

145. The FTC Act 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 Personal Information. The FTC publications and orders described above also formed part of the basis of Defendant's duty in this regard.

146. Defendant gathered and stored the Personal Information of Plaintiff and the Class as part of its business of soliciting and facilitating its services to its patients, which affect commerce.

147. Defendant violated the FTC Act by failing to use reasonable measures to protect the Personal Information of Plaintiff and the Class and by not complying with applicable industry standards, as described herein.

148. Defendant breached its duties to Plaintiff and the Class under the FTC Act, HIPAA, and the CCPA by failing to provide fair, reasonable, or adequate computer systems and/or data security practices to safeguard Plaintiff's and Class members' Personal Information, and by failing to provide prompt and specific notice without reasonable delay.

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

150. Plaintiff and the Class are within the class of persons that HIPAA and the FTC Act were intended to protect.

151. Defendant was required to comply with the CCPA, particularly as to Class members who are residents of California.

152. The harm that occurred as a result of the Data Breach is the type of harm the FTC Act, HIPAA, and CCPA were intended to guard against.

153. Defendant breached its duties to Plaintiff and the Class under these laws by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiff's and the Class's Personal Information.

154. Additionally, Defendant had a duty to promptly notify victims of the Data Breach. For instance, HIPAA required Defendant to notify victims of the Breach within sixty (60) days of the discovery of the Data Breach while Cal. Civ. Code §1798.82 required Defendant to issue breach notification "in the most expedient time possible and without unreasonable delay." Defendant did not begin notifying Plaintiff or Class members of the Data Breach until around July 9, 2021. Defendant, however, knew of the Data Breach by April 26, 2021.

155. Defendant breached its duties to Plaintiff and the Class by unreasonably delaying and failing to provide notice of the Data Breach expeditiously and/or as soon as practicable to Plaintiff and the Class.

156. Defendant's violations of the FTC Act, HIPAA, and the CCPA constitute negligence *per se*.

157. As a direct and proximate result of Defendant's negligence *per se*, Plaintiff and the Class have suffered, and continue to suffer, damages arising from the Data Breach, as alleged above.

158. The injury and harm that Plaintiff and Class members suffered (as alleged above) was the direct and proximate result of Defendant's negligence *per se*.

159. Plaintiff and the Class have suffered injury and are entitled to actual and punitive damages in amounts to be proven at trial.

B. COUNT II – INVASION OF PRIVACY

160. Plaintiff incorporates by reference all allegations of the preceding paragraphs as though fully set forth herein.

161. California established the right to privacy in Article 1, Section 1 of the California Constitution.

162. The State of California recognizes the tort of Intrusion into Private Affairs and adopts the formulation of that tort found in the Restatement (Second) of Torts, which states, "One who intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns is subject to liability to the other for invasion of his privacy if the intrusion would be highly offensive to a reasonable person." Restatement (Second) of Torts, § 652B (1977).

163. The state of North Carolina also recognizes the tort of Invasion of Privacy. *See Toomer v. Garrett*, 155 N.C. App. 462, 574 S.E.2d 76 (2002), *disc. rev. denied*, 357 N.C. 66, 579 S.E.2d 576 (2003).

164. Plaintiff and Class members had a legitimate and reasonable expectation of privacy with respect to their Personal Information and were accordingly entitled to the protection of this information against disclosure to and acquisition by unauthorized third parties.

165. Defendant owed a duty to its patients, including Plaintiff and Class members, to keep their Personal Information confidential.

166. The unauthorized access, acquisition, appropriation, disclosure, encumbrance, exfiltration, release, theft, use, and/or viewing of Personal Information, especially the type of information that is the subject of this action, is highly offensive to a reasonable person.

167. The intrusion was into a place or thing that was private and is entitled to be private. Plaintiff and Class members disclosed their Personal Information to Defendant as part of their receiving loan services for the payment of medical care, but privately, with the intention that such highly sensitive information would be kept confidential and protected from unauthorized access, acquisition, appropriation, disclosure, encumbrance, exfiltration, release, theft, use, and/or viewing. Plaintiff and Class members were reasonable in their belief that such information would be kept private and would not be disclosed without their authorization.

168. The Data Breach constitutes an intentional interference with Plaintiff's and Class members' interest in solitude or seclusion, either as to their persons or as to their private affairs or concerns, of a kind that would be highly offensive to a reasonable person.

169. Defendant acted with a knowing state of mind when it permitted the Data Breach because it knew its information security practices were inadequate.

170. Acting with knowledge, Defendant had notice and knew that its inadequate cybersecurity practices would cause injury to Plaintiff and Class members.

171. As a proximate result of Defendant's acts and omissions, Plaintiff's and Class members' Personal Information was accessed by, acquired by, appropriated by, disclosed to, encumbered by, exfiltrated by, released to, stolen

by, used by, and/ or reviewed by third parties without authorization, causing Plaintiff and Class members to suffer damages.

172. Unless and until enjoined and restrained by order of this Court, Defendant's wrongful conduct will continue to cause great and irreparable injury to Plaintiff and Class members in that the Personal Information maintained by Defendant can be acquired by, appropriated by, disclosed to, encumbered by, exfiltrated by, released to, stolen by, used by, accessed by, and/ or viewed by unauthorized persons.

173. Plaintiff and the Class have no adequate remedy at law for the injuries in that a judgment for monetary damages will not end the invasion of privacy for Plaintiff and Class members.

C. COUNT III – UNJUST ENRICHMENT

174. Plaintiff incorporates by reference all allegations of the preceding paragraphs as though fully set forth herein.

175. Plaintiff and the Class bring this claim in the alternative to all other claims and remedies at law.

176. Through and as a result of Plaintiff and Class members' use of Defendant's loan services, Defendant received monetary benefits.

177. Defendant collected, maintained, and stored the Personal Information of Plaintiff and Class members and, as such, Defendant had direct knowledge of the monetary benefits conferred upon it by Plaintiff's and Class members' use of Defendant's services.

178. Defendant, by way of its affirmative actions and omissions, including its knowing violations of its express or implied contracts with Plaintiff and the Class members, knowingly and deliberately enriched itself by saving the costs it reasonably and contractually should have expended on HIPAA and CCPA compliance and reasonable data privacy and security measures to secure Plaintiff's and Class members' Personal Information.

179. Instead of providing a reasonable level of security, training, and protocols that would have prevented the Data Breach, as described above and as is common industry practice among companies entrusted with similar Personal Information, Defendant, upon information and belief, instead consciously and opportunistically calculated to increase its own profits at the expense of Plaintiff and Class members.

180. As a direct and proximate result of Defendant's decision to profit rather than provide adequate data security, Plaintiff and Class members suffered and continue to suffer actual damages, including (i) the amount of the savings and costs Defendant reasonably and contractually should have expended on data security measures to secure Plaintiff's Personal Information, (ii) time and expenses mitigating harms, (iii) diminished value of Personal Information, (iv) loss of privacy, (v) harms as a result of identity theft; and (vi) an increased risk of future identity theft.

181. Defendant, upon information and belief, has therefore engaged in opportunistic, unethical, and immoral conduct by profiting from conduct that it knew would create a significant and highly likely risk of substantial and certainly impending harm to Plaintiff and the Class in direct violation of Plaintiff's and Class members' legally protected interests. As such, it would be inequitable, unconscionable, and unlawful to permit Defendant to retain the benefits it derived as a consequence of its wrongful conduct.

182. Accordingly, Plaintiff and the Class are entitled to relief in the form of restitution and disgorgement of all ill-gotten gains, which should be put into a common fund to be distributed to Plaintiff and the Class.

D. COUNT IV – BREACH OF CONTRACT

183. Plaintiff incorporates by reference all allegations of the preceding paragraphs as though fully set forth herein.

184. Plaintiff and the Class entered into contracts with Defendant, under which Defendant received payments in exchange for Plaintiff and Class members' use of Defendant's loan services.

185. The promises and representations described above relating to the use of industry practices and Defendant's concern for its customers' privacy rights, became terms of the contract between Defendant and its customers, including Plaintiff and the Class.

186. Defendant breached these promises by failing to comply with reasonable industry practices, including established under HIPAA, the FTC Act, and the CCPA.

187. As a result of Defendant's breach of these terms, Plaintiff and the Class have been seriously harmed and put at grave risk of debilitating future harms.

188. Plaintiff and Class members are therefore entitled to damages in an amount to be determined at trial.

E. COUNT V – BREACH OF IMPLIED CONTRACT (ALTERNATIVELY TO COUNT IV)

189. Plaintiff incorporates by reference all allegations of the preceding paragraphs as though fully set forth herein.

190. When Plaintiff and the Class members provided their Personal Information to Defendant when seeking loans for the payment of medical services, they entered into implied contracts in which Defendant agreed to comply with its statutory and common law duties to protect Plaintiff's and Class members' Personal Information and to timely notify them in the event of a data breach.

191. Defendant required Plaintiff and Class members to provide, or authorize the transfer of, their Personal Information in order for them to receive loans for the payment of medical services and treatments.

192. Based on the implicit understanding and also on Defendant's representations (as described above), Plaintiff and the Class accepted Defendant's offers and provided Defendant with their Personal Information.

193. Plaintiff and Class members would not have provided their Personal Information to Defendant had they known that Defendant would not safeguard their Personal Information, as promised, or provide timely notice of a data breach.

194. Plaintiff and Class members fully performed their obligations under their implied contracts with Defendant.

195. Defendant breached the implied contracts by failing to safeguard Plaintiff's and Class members' Personal Information and by failing to provide them with timely and accurate notice of the Data Breach.

196. The losses and damages Plaintiff and Class members sustained (as described above) were the direct and proximate result of Defendant's breach of its implied contracts with Plaintiff and Class members.

F. COUNT VI – BREACH OF CONFIDENCE

197. Plaintiff incorporates by reference all allegations of the preceding paragraphs as though fully set forth herein.

198. Defendant was fully aware of the confidential nature of the Personal Information that Plaintiff and Class members provided to Defendant.

199. As alleged herein and above, Defendant's relationship with Plaintiff and the Class was governed by promises and expectations that Plaintiff and Class members' Personal Information would be collected, stored, and protected in confidence, and would not be accessed by, acquired by, appropriated by, disclosed to, encumbered by, exfiltrated by, released to, stolen by, used by, and/or viewed by unauthorized third parties.

200. Plaintiff and Class members provided their respective Personal Information to Defendant with the explicit and implicit understandings that Defendant would protect the Personal Information and not permit it to be accessed

by, acquired by, appropriated by, disclosed to, encumbered by, exfiltrated by, released to, stolen by, used by, and/or viewed by unauthorized third parties.

201. Plaintiff and Class members also provided their Personal Information to Defendant with the explicit and implicit understanding that Defendant would take precautions to protect their Personal Information from unauthorized access, acquisition, appropriation, disclosure, encumbrance, exfiltration, release, theft, use, access, and/or viewing by following basic principles of protecting its networks, data systems, and employee business email accounts.

202. Defendant voluntarily received, in confidence, Plaintiff's and Class members' Personal Information with the understanding that the Personal Information would not be accessed by, acquired by, appropriated by, disclosed to, encumbered by, exfiltrated by, released to, stolen by, used by, and/or viewed by the public or any unauthorized third parties.

203. Due to Defendant's failure to prevent the Data Breach from occurring and detect the Data Breach after it occurred by, inter alia, not following best information security practices to secure Plaintiff's and Class members' Personal Information, Plaintiff's and Class members' Personal Information was accessed by, acquired by, appropriated by, disclosed to, encumbered by, exfiltrated by, released to, stolen by, used by, and/or viewed by unauthorized third parties beyond Plaintiff's and Class members' confidence, and without their express permission.

204. As a direct and proximate cause of Defendant's actions and/or omissions, Plaintiff and Class members have suffered damages as alleged herein.

205. But for Defendant's failure to maintain and protect Plaintiff's and Class members' Personal Information in violation of the parties' understanding of confidence, their Personal Information would not have been accessed by, acquired by, appropriated by, disclosed to, encumbered by, exfiltrated by, released to, stolen by, used by, and/or viewed by unauthorized third parties. Defendant's Data

Breach was the direct and legal cause of the misuse of Plaintiff's and Class members' Personal Information, as well as the resulting damages.

206. The injury and harm Plaintiff and Class members suffered and will continue to suffer was the reasonably foreseeable result of Defendant's unauthorized misuse of Plaintiff's and Class members' Personal Information. Defendant knew its data systems and protocols for accepting and securing Plaintiff's and Class members' Personal Information had security and other vulnerabilities that placed Plaintiff's and Class members' Personal Information in jeopardy.

207. As a direct and proximate result of Defendant's breaches of confidence, Plaintiff and Class members have suffered and will suffer injury, as alleged herein, including but not limited to (a) actual identity theft; (b) the compromise, publication, and/or theft of their Personal Information; (c) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft and/or unauthorized use of their Personal Information; (d) 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 identity theft; (e) the continued risk to their Personal 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 Class Members' Personal Information in their continued possession; and (f) future costs in terms of time, effort, and money that will be expended as result of the Data Breach for the remainder of the lives of Plaintiff and Class Members.

G. COUNT VII – BREACH OF IMPLIED COVENANT OF GOOD FAITH AND FAIR DEALING

208. Plaintiff incorporates by reference all allegations of the preceding paragraphs as though fully set forth herein.

209. As described above, Defendant made promises and representations to Plaintiff and the Class that it would comply with industry standard practices.

210. These promises and representations became a part of the contract between Defendant and Plaintiff and the Class.

211. While Defendant had discretion in the specifics of how it met the applicable laws and industry standards, this discretion was governed by an implied covenant of good faith and fair dealing.

212. Defendant breached this implied covenant when it engaged in acts and/or omissions that are declared unfair trade practices by the FTC and state statutes and regulations (including those in California and North Carolina), and when it engaged in unlawful practices under HIPAA, the FTC, the CCPA, and other state privacy laws. These acts and omissions included: representing that it would maintain adequate data privacy and security practices and procedures to safeguard the Personal Information from unauthorized disclosures, releases, data breaches, and theft; omitting, suppressing, and concealing the material fact of the inadequacy of the privacy and security protections for the Class's Personal Information; and failing to disclose to the Class at the time they provided their Personal Information to Defendant that its data security systems and protocols, including training, auditing, and testing of employees, failed to meet applicable legal and industry standards.

213. Plaintiff and Class members did all or substantially all the significant things that the contract required them to do.

214. Likewise, all conditions required for Defendant's performance were met.

215. Defendant's acts and omissions unfairly interfered with Plaintiff's and Class members' rights to receive the full benefit of their contracts.

216. Plaintiff and Class members have been harmed by Defendant's breach of this implied covenant in the many ways described above, including actual identity theft, imminent risk of certainly impending and devastating identity theft that exists now that cyber criminals have their Personal Information, and the attendant long-term time and expenses spent attempting to mitigate and insure against these risks.

217. Defendant is liable for this breach of these implied covenants, whether or not it is found to have breached any specific express contractual term.

218. Plaintiff and Class members are entitled to damages, including compensatory damages and restitution, declaratory and injunctive relief, and attorney fees, costs, and expenses.

H. COUNT VIII – VIOLATIONS OF CALIFORNIA UNFAIR COMPETITION LAW, Cal. Bus. & Prof. Code §17200, *et seq.*

219. Plaintiff incorporates by reference all allegations of the preceding paragraphs as though fully set forth herein.

220. Plaintiff brings this Count against Defendant on behalf of the Class.

221. Defendant violated California's Unfair Competition Law ("UCL"), Cal. Bus. Prof. Code § 17200, *et seq.*, by engaging in unlawful, unfair or fraudulent business acts and practices and unfair, deceptive, untrue or misleading advertising that constitute acts of "unfair competition" as defined in the UCL, including, but not limited to, the following:

a. by representing and advertising that it would maintain adequate data privacy and security practices and procedures to safeguard Plaintiff's and Class members' Personal Information from unauthorized disclosure, release, data breach, and theft; representing and advertising that it did and would comply with

the requirement of relevant federal and state laws pertaining to the privacy and security of the Class's Personal Information; and omitting, suppressing, and concealing the material fact of the inadequacy of the privacy and security protections for the Class's Personal Information;

b. by soliciting and collecting Class members' Personal Information with knowledge that the information would not be adequately protected; and by storing Plaintiff's and Class members' Personal Information in an unsecure and unencrypted electronic environment;

c. by failing to disclose the Data Breach in a timely and accurate manner, in violation of Cal. Civ. Code §1798.82;

d. by violating the privacy and security requirements of HIPAA, 42 U.S.C. §1302d, *et seq.*; and

e. by violating the CCPA, Cal. Civ. Code § 1798.81.5.

222. These unfair acts and practices were immoral, unethical, oppressive, unscrupulous, unconscionable, and/or substantially injurious to Plaintiff and Class members. Defendant's practices were also contrary to legislatively declared and public policies that seek to protect consumer data and ensure that entities that solicit or are entrusted with personal data utilize appropriate security measures, as reflected by laws like the FTC Act, 15 U.S.C. § 45, HIPAA, 42 U.S.C. § 1302d, *et seq.*, and the CCPA, Cal. Civ. Code § 1798.81.5.

223. As a direct and proximate result of Defendant's unfair and unlawful practices and acts, Plaintiff and the Class were injured and lost money or property, including but not limited to the overpayments Defendant received to take reasonable and adequate security measures (but did not), the loss of their legally protected interest in the confidentiality and privacy of their Personal Information, and additional losses described above.

224. Defendant knew or should have known that its systems, email accounts, and data security practices were inadequate to safeguard Plaintiff's and Class members' Personal Information and that the risk of a data breach or theft was highly likely. Defendant's actions in engaging in the above-named unfair practices and deceptive acts were negligent, knowing and willful, and/or wanton and reckless with respect to the rights of the Class.

225. Plaintiff seeks relief under the UCL, including restitution to the Class of money or property that the Defendant may have acquired by means of Defendant's deceptive, unlawful, and unfair business practices, declaratory relief, attorney fees, costs and expenses (pursuant to Cal. Code Civ. P. § 1021.5), and injunctive or other equitable relief.

I. COUNT IX – NORTH CAROLINA DECEPTIVE TRADE PRACTICES ACT, N.C. Gen. Stat. § 75-1.1, *et seq.* (on Behalf of an Alternative North Carolina Class)

226. Plaintiff incorporates by reference all allegations of the preceding paragraphs as though fully set forth herein.

227. Plaintiff brings this claim against Defendant on behalf of an alternative North Carolina Class.

228. North Carolina law declares unlawful all "unfair or deceptive acts or practices in or affecting commerce" N.C. Gen. Stat. § 75-1.1.

229. "Commerce" is defined broadly as any business activity other than "professional services rendered by a members of a learned profession." *Id.*

230. The North Carolina Identity Theft Protection Act required Defendant to provide individual notice to Breach Victims "without unreasonable delay." N.C. Gen. Stat. § 75-65(a).

231. By failing to provide individual notice within 60 days of discovering the Breach, as required under the HIPAA Notification Rule, Defendant's delay was unreasonable.

232. Plaintiff was injured by this delay because, immediately following the Breach period, Plaintiff began receiving notifications of attempts to open credit cards in her name and also recently learned that someone has fraudulently opened a bank account in her name. These experiences have resulted in significant distress and anxiety. She was also prevented from protecting herself sooner. Other members of the alternative North Carolina Class were similarly injured.

233. Defendant engaged in unlawful, unfair, and deceptive acts and practices, misrepresentations, and the concealment, suppression, and omission of material facts with respect to the sale and advertisement of the services used by Plaintiff and the alternative North Carolina Class in violation of N.C. Gen. Stat. § 75-1.1, including but not limited to the following:

a. Defendant omitted, suppressed, and concealed the material fact of the inadequacy of the privacy and security protections for the alternative North Carolina Class's Personal Information;

b. Defendant engaged in unfair, unlawful, and deceptive acts and practices with respect to its loan services by failing to maintain the privacy and security of the alternative North Carolina Class's Personal Information, in violation of duties imposed by and public policies reflected in applicable federal and state laws, resulting in the Data Breach. These unfair, unlawful, and deceptive acts and practices violated duties imposed by laws including the FTC Act, 15 U.S.C. § 45 and HIPAA, 42 U.S.C. § 1302d, *et seq.*;

c. Defendant engaged in unlawful, unfair, and deceptive acts and practices with respect to its loan services by failing to disclose the Data Breach to the alternative North Carolina Class in a timely and accurate manner; and

d. Defendant engaged in unlawful, unfair, and deceptive acts and practices with respect to its loans services by failing to take proper action following the Data Breach to enact adequate privacy and security measures and protect the alternative North Carolina Class' Personal Information from further unauthorized disclosure, release, data breach, and theft.

234. The above unlawful, unfair, and deceptive acts and practices by Defendant were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury to consumers that the consumers could not reasonably avoid; this substantial injury outweighed any benefits to consumers or to competition.

235. Defendant knew or should have known that its computer systems, email accounts, and data security practices were inadequate to safeguard the alternative subclass's Personal Information and that risk of a data breach or theft was highly likely. Defendant's actions in engaging in the above-named deceptive acts and practices were negligent, knowing and willful, and/or wanton and reckless with respect to the rights of members of the alternative North Carolina Class.

236. As a direct and proximate result of Defendant's deceptive acts and practices, the alternative North Carolina Class members suffered an ascertainable loss, as described above, including the loss of their legally protected interest in the confidentiality and privacy of their Personal Information.

237. Individuals injured by unfair or deceptive acts or practices are entitled to treble damages. N.C. Gen. Stat. § 75-16.

238. Plaintiff and the alternative subclass seek relief under N.C. Gen. Stat. §§ 75-1.1, *et seq.*, and request treble damages, attorney fees, expenses, and costs, and injunctive relief.

J. COUNT X – DECLARATORY RELIEF

239. Plaintiff incorporates by reference all allegations of the preceding paragraphs as though fully set forth herein.

240. Plaintiff brings this Count under the federal Declaratory Judgment Act, 28 U.S.C. §2201.

241. As previously alleged, Plaintiff and members of the Class entered into an implied contract that required Defendant to provide adequate security for the Personal Information it collected from Plaintiff and the Class.

242. Defendant owes a duty of care to Plaintiff and the members of the Class that requires them to adequately secure Personal Information.

243. Defendant still possesses Personal Information regarding Plaintiff and members of the Class.

244. Since the Data Breach, Defendant has announced few if any changes to its data security infrastructure, processes or procedures to fix the vulnerabilities in its computer and email systems and/or security practices which permitted the Data Breach to occur and go undetected for months and, thereby, prevent further attacks.

245. Defendant has not satisfied its contractual obligations and legal duties to Plaintiff and the Class. In fact, now that Defendant's insufficient data security is known to hackers, the Personal Information in Defendant's possession is even more vulnerable to cyberattack.

246. Actual harm has arisen in the wake of the Data Breach regarding Defendant's contractual obligations and duties of care to provide security measures to Plaintiff and the members of the Class. Further, Plaintiff and the members of the Class are at risk of additional or further harm due to the exposure of its Personal Information and Defendant's failure to address the security failings that lead to such exposure.

247. There is no reason to believe that Defendant's security measures are more adequate to meet its contractual obligations and legal duties now than they were before the Breach.

248. Plaintiff, therefore, seeks a declaration that Defendant's existing security measures do not comply with its contractual obligations and duties of care to provide adequate security and that to comply with its contractual obligations and duties of care, Defendant must implement and maintain additional security measures.

VIII. PRAYER FOR RELIEF

WHEREFORE, Plaintiff and the Class pray for judgment against Defendant as follows:

a. An order certifying this action as a class action under Fed. R. Civ. P. 23, defining the Class as requested herein, appointing the undersigned as Class counsel, and finding that Plaintiff is a proper representative of the Class requested herein;

b. A judgment in favor of Plaintiff and the Class awarding them appropriate monetary relief, including actual and statutory damages, punitive damages, attorney fees, expenses, costs, and such other and further relief as is just and proper.

c. An order providing injunctive and other equitable relief as necessary to protect the interests of the Class and the general public as requested herein, including, but not limited to:

i. Ordering that Defendant engage third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis, and ordering Defendant to

promptly correct any problems or issues detected by such third-party security auditors;

ii. Ordering that Defendant engage third-party security auditors and internal personnel to run automated security monitoring;

iii. Ordering that Defendant audit, test, and train its security personnel regarding any new or modified procedures;

iv. Ordering that Defendant segment customer data by, among other things, creating firewalls and access controls so that if one area of Defendant's systems is compromised, hackers cannot gain access to other portions of Defendant's systems;

v. Ordering that Defendant cease transmitting Personal Information via unencrypted email;

vi. Ordering that Defendant cease storing Personal Information in email accounts;

vii. Ordering that Defendant purge, delete, and destroy in a reasonably secure manner customer data not necessary for its provisions of services;

viii. Ordering that Defendant conduct regular database scanning and securing checks;

ix. Ordering that Defendant routinely and continually conduct internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach; and

x. Ordering Defendant to meaningfully educate its current, former, and prospective employees and subcontractors

about the threats faced as a result of the loss of financial and personal information to third parties, as well as the steps they must take to protect against such occurrences;

d. An order requiring Defendant to pay the costs involved in notifying the Class members about the judgment and administering the claims process;

e. A judgment in favor of Plaintiff and the Class awarding them pre-judgment and post-judgment interest, reasonable attorneys' fees, costs and expenses as allowable by law; and

f. An award of such other and further relief as this Court may deem just and proper.

IX. DEMAND FOR JURY TRIAL

Plaintiff demands a trial by jury on all issues so triable.

DATED: July 27, 2021

FELL LAW, P.C.

By: /s/ Bibianne U. Fell
Bibianne U. Fell

Bibianne U. Fell (State Bar No. 234194)
l1956 Bernardo Plaza Dr. #53l,
San Diego, CA 92128
Telephone: (858) 201-3960
Email: bibi@fellfirm.com

William B. Federman*
FEDERMAN & SHERWOOD
10205 N. Pennsylvania Ave.
Oklahoma City, OK 73120
Telephone: (405) 235-1560
Email: wbf@federmanlaw.com
**Pro Hac Vice application to be submitted*

Counsel for Plaintiff and the Proposed Class

JS 44 (Rev. 10/20)

CIVIL COVER SHEET

The JS 44 civil cover sheet and the information contained herein neither replace nor supplement the filing and service of pleadings or other papers as required by law, except as provided by local rules of court. This form, approved by the Judicial Conference of the United States in September 1974, is required for the use of the Clerk of Court for the purpose of initiating the civil docket sheet. *(SEE INSTRUCTIONS ON NEXT PAGE OF THIS FORM.)*

I. (a) PLAINTIFFS

BROOKE ROBERTS-GOODEN, individually and on behalf of all others similarly situated

(b) County of Residence of First Listed Plaintiff Mecklenburg
(EXCEPT IN U.S. PLAINTIFF CASES)

(c) Attorneys *(Firm Name, Address, and Telephone Number)*
Bibianne U. Fell, Esq. FELL LAW, P.C.
11956 Bernardo Plaza Dr.#531, San Diego, CA 92128
(858) 201-3960

DEFENDANTS

CSI FINANCIAL SERVICES, LLC, d/b/a CLEARBALANCE HOLDINGS, LLC

County of Residence of First Listed Defendant San Diego
(IN U.S. PLAINTIFF CASES ONLY)

NOTE: IN LAND CONDEMNATION CASES, USE THE LOCATION OF THE TRACT OF LAND INVOLVED.

Attorneys *(If Known)*

'21CV1352 BAS BGS

II. BASIS OF JURISDICTION *(Place an "X" in One Box Only)*

- ☐ 1 U.S. Government Plaintiff
- ☐ 3 Federal Question *(U.S. Government Not a Party)*
- ☐ 2 U.S. Government Defendant
- ☒ 4 Diversity *(Indicate Citizenship of Parties in Item III)*

III. CITIZENSHIP OF PRINCIPAL PARTIES *(Place an "X" in One Box for Plaintiff and One Box for Defendant)*
(For Diversity Cases Only)

	PTF	DEF		PTF	DEF
Citizen of This State	☐ 1	☐ 1	Incorporated *or* Principal Place of Business In This State	☐ 4	☒ 4
Citizen of Another State	☒ 2	☐ 2	Incorporated *and* Principal Place of Business In Another State	☐ 5	☐ 5
Citizen or Subject of a Foreign Country	☐ 3	☐ 3	Foreign Nation	☐ 6	☐ 6

IV. NATURE OF SUIT *(Place an "X" in One Box Only)*

Click here for: Nature of Suit Code Descriptions.

CONTRACT
- ☐ 110 Insurance
- ☐ 120 Marine
- ☐ 130 Miller Act
- ☐ 140 Negotiable Instrument
- ☐ 150 Recovery of Overpayment & Enforcement of Judgment
- ☐ 151 Medicare Act
- ☐ 152 Recovery of Defaulted Student Loans (Excludes Veterans)
- ☐ 153 Recovery of Overpayment of Veteran's Benefits
- ☐ 160 Stockholders' Suits
- DF ☒ 190 Other Contract
- ☐ 195 Contract Product Liability
- ☐ 196 Franchise

REAL PROPERTY
- ☐ 210 Land Condemnation
- ☐ 220 Foreclosure
- ☐ 230 Rent Lease & Ejectment
- ☐ 240 Torts to Land
- ☐ 245 Tort Product Liability
- ☐ 290 All Other Real Property

TORTS

PERSONAL INJURY
- ☐ 310 Airplane
- ☐ 315 Airplane Product Liability
- ☐ 320 Assault, Libel & Slander
- ☐ 330 Federal Employers' Liability
- ☐ 340 Marine
- ☐ 345 Marine Product Liability
- ☐ 350 Motor Vehicle
- ☐ 355 Motor Vehicle Product Liability
- ☐ 360 Other Personal Injury
- ☐ 362 Personal Injury - Medical Malpractice

PERSONAL INJURY
- ☐ 365 Personal Injury - Product Liability
- ☐ 367 Health Care/ Pharmaceutical Personal Injury Product Liability
- ☐ 368 Asbestos Personal Injury Product Liability

PERSONAL PROPERTY
- ☐ 370 Other Fraud
- ☐ 371 Truth in Lending
- ☐ 380 Other Personal Property Damage
- ☐ 385 Property Damage Product Liability

CIVIL RIGHTS
- ☐ 440 Other Civil Rights
- ☐ 441 Voting
- ☐ 442 Employment
- ☐ 443 Housing/ Accommodations
- ☐ 445 Amer. w/Disabilities - Employment
- ☐ 446 Amer. w/Disabilities - Other
- ☐ 448 Education

PRISONER PETITIONS

Habeas Corpus:
- ☐ 463 Alien Detainee
- ☐ 510 Motions to Vacate Sentence
- ☐ 530 General
- ☐ 535 Death Penalty

Other:
- ☐ 540 Mandamus & Other
- ☐ 550 Civil Rights
- ☐ 555 Prison Condition
- ☐ 560 Civil Detainee - Conditions of Confinement

FORFEITURE/PENALTY
- ☐ 625 Drug Related Seizure of Property 21 USC 881
- ☐ 690 Other

LABOR
- ☐ 710 Fair Labor Standards Act
- ☐ 720 Labor/Management Relations
- ☐ 740 Railway Labor Act
- ☐ 751 Family and Medical Leave Act
- ☐ 790 Other Labor Litigation
- ☐ 791 Employee Retirement Income Security Act

IMMIGRATION
- ☐ 462 Naturalization Application
- ☐ 465 Other Immigration Actions

BANKRUPTCY
- ☐ 422 Appeal 28 USC 158
- ☐ 423 Withdrawal 28 USC 157

PROPERTY RIGHTS
- ☐ 820 Copyrights
- ☐ 830 Patent
- ☐ 835 Patent - Abbreviated New Drug Application
- ☐ 840 Trademark
- ☐ 880 Defend Trade Secrets Act of 2016

SOCIAL SECURITY
- ☐ 861 HIA (1395ff)
- ☐ 862 Black Lung (923)
- ☐ 863 DIWC/DIWW (405(g))
- ☐ 864 SSID Title XVI
- ☐ 865 RSI (405(g))

FEDERAL TAX SUITS
- ☐ 870 Taxes (U.S. Plaintiff or Defendant)
- ☐ 871 IRS—Third Party 26 USC 7609

OTHER STATUTES
- ☐ 375 False Claims Act
- ☐ 376 Qui Tam (31 USC 3729(a))
- ☐ 400 State Reapportionment
- ☐ 410 Antitrust
- ☐ 430 Banks and Banking
- ☐ 450 Commerce
- ☐ 460 Deportation
- ☐ 470 Racketeer Influenced and Corrupt Organizations
- ☐ 480 Consumer Credit (15 USC 1681 or 1692)
- ☐ 485 Telephone Consumer Protection Act
- ☐ 490 Cable/Sat TV
- ☐ 850 Securities/Commodities/ Exchange
- ☒ 890 Other Statutory Actions
- ☐ 891 Agricultural Acts
- ☐ 893 Environmental Matters
- ☐ 895 Freedom of Information Act
- ☐ 896 Arbitration
- ☐ 899 Administrative Procedure Act/Review or Appeal of Agency Decision
- ☐ 950 Constitutionality of State Statutes

V. ORIGIN *(Place an "X" in One Box Only)*

☒ 1 Original Proceeding | ☐ 2 Removed from State Court | ☐ 3 Remanded from Appellate Court | ☐ 4 Reinstated or Reopened | ☐ 5 Transferred from Another District *(specify)* | ☐ 6 Multidistrict Litigation - Transfer | ☐ 8 Multidistrict Litigation - Direct File

VI. CAUSE OF ACTION

Cite the U.S. Civil Statute under which you are filing ***(Do not cite jurisdictional statutes unless diversity)***:
28 U.S.C. § 1332(d)

Brief description of cause:
Data Breach

VII. REQUESTED IN COMPLAINT:

☒ CHECK IF THIS IS A **CLASS ACTION** UNDER RULE 23, F.R.Cv.P.

DEMAND $

CHECK YES only if demanded in complaint:
JURY DEMAND: ☒ Yes ☐ No

VIII. RELATED CASE(S) IF ANY

(See instructions): JUDGE _____ DOCKET NUMBER _____

DATE
Jul 27, 2021

SIGNATURE OF ATTORNEY OF RECORD
Bibianne U Fell

FOR OFFICE USE ONLY

RECEIPT # _____ AMOUNT _____ APPLYING IFP _____ JUDGE _____ MAG. JUDGE _____

INSTRUCTIONS FOR ATTORNEYS COMPLETING CIVIL COVER SHEET FORM JS 44

Authority For Civil Cover Sheet

The JS 44 civil cover sheet and the information contained herein neither replaces nor supplements the filings and service of pleading or other papers as required by law, except as provided by local rules of court. This form, approved by the Judicial Conference of the United States in September 1974, is required for the use of the Clerk of Court for the purpose of initiating the civil docket sheet. Consequently, a civil cover sheet is submitted to the Clerk of Court for each civil complaint filed. The attorney filing a case should complete the form as follows:

I.(a) **Plaintiffs-Defendants.** Enter names (last, first, middle initial) of plaintiff and defendant. If the plaintiff or defendant is a government agency, use only the full name or standard abbreviations. If the plaintiff or defendant is an official within a government agency, identify first the agency and then the official, giving both name and title.

(b) **County of Residence.** For each civil case filed, except U.S. plaintiff cases, enter the name of the county where the first listed plaintiff resides at the time of filing. In U.S. plaintiff cases, enter the name of the county in which the first listed defendant resides at the time of filing. (NOTE: In land condemnation cases, the county of residence of the "defendant" is the location of the tract of land involved.)

(c) **Attorneys.** Enter the firm name, address, telephone number, and attorney of record. If there are several attorneys, list them on an attachment, noting in this section "(see attachment)".

II. **Jurisdiction.** The basis of jurisdiction is set forth under Rule 8(a), F.R.Cv.P., which requires that jurisdictions be shown in pleadings. Place an "X" in one of the boxes. If there is more than one basis of jurisdiction, precedence is given in the order shown below.
United States plaintiff. (1) Jurisdiction based on 28 U.S.C. 1345 and 1348. Suits by agencies and officers of the United States are included here.
United States defendant. (2) When the plaintiff is suing the United States, its officers or agencies, place an "X" in this box.
Federal question. (3) This refers to suits under 28 U.S.C. 1331, where jurisdiction arises under the Constitution of the United States, an amendment to the Constitution, an act of Congress or a treaty of the United States. In cases where the U.S. is a party, the U.S. plaintiff or defendant code takes precedence, and box 1 or 2 should be marked.
Diversity of citizenship. (4) This refers to suits under 28 U.S.C. 1332, where parties are citizens of different states. When Box 4 is checked, the citizenship of the different parties must be checked. (See Section III below**; NOTE: federal question actions take precedence over diversity cases.**)

III. **Residence (citizenship) of Principal Parties.** This section of the JS 44 is to be completed if diversity of citizenship was indicated above. Mark this section for each principal party.

IV. **Nature of Suit.** Place an "X" in the appropriate box. If there are multiple nature of suit codes associated with the case, pick the nature of suit code that is most applicable. Click here for: Nature of Suit Code Descriptions.

V. **Origin.** Place an "X" in one of the seven boxes.
Original Proceedings. (1) Cases which originate in the United States district courts.
Removed from State Court. (2) Proceedings initiated in state courts may be removed to the district courts under Title 28 U.S.C., Section 1441.
Remanded from Appellate Court. (3) Check this box for cases remanded to the district court for further action. Use the date of remand as the filing date.
Reinstated or Reopened. (4) Check this box for cases reinstated or reopened in the district court. Use the reopening date as the filing date.
Transferred from Another District. (5) For cases transferred under Title 28 U.S.C. Section 1404(a). Do not use this for within district transfers or multidistrict litigation transfers.
Multidistrict Litigation – Transfer. (6) Check this box when a multidistrict case is transferred into the district under authority of Title 28 U.S.C. Section 1407.
Multidistrict Litigation – Direct File. (8) Check this box when a multidistrict case is filed in the same district as the Master MDL docket.
PLEASE NOTE THAT THERE IS NOT AN ORIGIN CODE 7. Origin Code 7 was used for historical records and is no longer relevant due to changes in statue.

VI. **Cause of Action.** Report the civil statute directly related to the cause of action and give a brief description of the cause. **Do not cite jurisdictional statutes unless diversity.** Example: U.S. Civil Statute: 47 USC 553 Brief Description: Unauthorized reception of cable service.

VII. **Requested in Complaint.** Class Action. Place an "X" in this box if you are filing a class action under Rule 23, F.R.Cv.P.
Demand. In this space enter the actual dollar amount being demanded or indicate other demand, such as a preliminary injunction.
Jury Demand. Check the appropriate box to indicate whether or not a jury is being demanded.

VIII. **Related Cases.** This section of the JS 44 is used to reference related pending cases, if any. If there are related pending cases, insert the docket numbers and the corresponding judge names for such cases.

Date and Attorney Signature. Date and sign the civil cover sheet.

ClassAction.org