POTTER HANDY LLP
Mark D. Potter (SBN 166317)
mark@potterhandy.com
James M. Treglio (SBN 228077)
jimt@potterhandy.com
100 Pine St., Ste 1250
San Francisco, CA 94111
Tel: (415) 534-1911
Fax: (888) 422-5191

Attorneys for Plaintiffs Christopher Newton, Christa Vital, Scott Schutza, on behalf of themselves and all others similarly situated,

SUPERIOR COURT OF THE STATE OF CALIFORNIA

FOR THE COUNTY OF ALAMEDA

24CV073453

CHRISTOPHER NEWTON, CHRISTA VITAL, SCOTT SCHUTZA on behalf of themselves and all others similarly situated,

Plaintiffs,

vs.

KAISER FOUNDATION HEALTH PLAN, INC., a California Corporation; and DOES 1 through 100, inclusive,

Defendants.

CLASS ACTION

CLASS COMPLAINT FOR DAMAGES AND INJUNCTIVE RELIEF (FOR VIOLATIONS OF:

(1) THE CONFIDENTIALITY OF MEDICAL INFORMATION ACT, CIVIL CODE §§ 56, *ET SEQ.*);
(2) CALIFORNIA UNFAIR COMPETITION LAW, Cal. Bus. & Prof. Code §17200, *et seq.*;
(3) NEGLIGENCE; and
(4) NEGLIGENCE PER SE.

DEMAND FOR JURY TRIAL

Class Representative Plaintiffs Christopher Newton, Christa Vital, and Scott Schutza ("Plaintiffs"), by and through their attorneys, individually and on behalf of others similarly situated, allege upon information and belief as follows:

I.

INTRODUCTION

1. Under the Confidentiality of Medical Information Act, Civil Code §§ 56, *et seq.* (hereinafter referred to as the "Act"), Plaintiffs Christopher Newton, Christa Vital, Scott Schutza and all other persons similarly situated, had a right to keep their personal medical information provided to Defendant KAISER FOUNDATION HEALTH PLAN, INC. ("Kaiser" or "Defendant") confidential. The short title of the Act states, "The Legislature hereby finds and declares that persons receiving health care services have a right to expect that the confidentiality of individual identifiable medical information derived by health service providers be reasonably preserved. It is the intention of the Legislature in enacting this act, to provide for the confidentiality of individually identifiable medical information, while permitting certain reasonable and limited uses of that information." The Act specifically provides that "a provider of health care, health care service plan, or contractor shall not disclose medical information regarding a patient of the provider of health care or an enrollee or subscriber of a health care service plan without first obtaining an authorization...." Civil Code. § 56.10(a). The Act further provides that "Every provider of health care, health care service plan, pharmaceutical company, or contractor who creates, maintains, preserves, stores, abandons, destroys, or disposes of medical records shall do so in a manner that preserves the confidentiality of the information contained therein. Any provider of health care, health care service plan, pharmaceutical company, or contractor who negligently creates, maintains, preserves, stores, abandons, destroys, or disposes of medical records shall be subject to the remedies ... provided under subdivisions (b) ... of Section 56.36." Civil Code § 56.101(a).

2. Civil Code § 56.36(b) provides Plaintiffs, and all other persons similarly situated, with a private right to bring an action against Defendant for violation of Civil Code § 56.101 by specifically providing that "[i]n addition to any other remedies available at law, any individual may

bring an action against any person or entity who has negligently released confidential information or records concerning him or her in violation of this part, for either or both of the following: (1) ... nominal damages of one thousand dollars ($1,000). In order to recover under this paragraph, *it shall not be necessary that the plaintiff suffered or was threatened with actual damages*. (2) The amount of actual damages, if any, sustained by the patient." (Emphasis added.) Here, the release of information to third parties without so much as a subpoena clearly violates the requirements of this statute.

3. This class action is brought on behalf of Plaintiffs and a putative class defined as all patients of Defendant who received treatment at one of Defendant's hospital, satellite, or urgent care locations and whose personal medical information were released to third parties without authorization ("the "Class," or the "Class Members").

4. As alleged more fully below, Defendant created, maintained, preserved, and stored Plaintiffs and the Class members' personal medical information onto the Defendant's computer network, including websites and web applications prior to April 2024. Due to Defendant's intentional release of information without authorization, there was an unauthorized release of Plaintiffs' and the Class members' confidential medical information that occurred continuously from the time this information was provided by the Class to Defendant, in violation of Civil Code § 56.101 of the Act.

5. As alleged more fully below, Defendant created, maintained, preserved, and stored Plaintiffs' and the Class members' confidential medical information which were released to unauthorized persons, without Plaintiffs' and the Class members' prior written authorization. This act of providing unauthorized access to Plaintiffs' and the Class Members' confidential medical information continuously constitutes an unauthorized release of confidential medical information in violation of Civil Code § 56.101 of the Act. Because Civil Code § 56.101 allows for the remedies and penalties provided under Civil Code § 56.36(b), Class Representative Plaintiffs, individually and on behalf of others similarly situated, seek nominal damages of one thousand dollars ($1,000) for each violation under Civil Code § 56.36(b)(1). Additionally, Class Representative Plaintiffs,

individually and on behalf of others similarly situated, seek injunctive relief for unlawful violations of Business and Professions Code §§ 17200, *et seq*.

6. Class Representative Plaintiffs do not seek any relief greater than or different from the relief sought for the Class of which Plaintiffs are members. The action, if successful, will enforce an important right affecting the public interest and would confer a significant benefit, whether pecuniary or non-pecuniary, for a large class of persons. Private enforcement is necessary and places a disproportionate financial burden on Class Representative Plaintiffs in relation to Class Representative Plaintiffs' stake in the matter.

II.

JURISDICTION AND VENUE

7. This Court has jurisdiction over this action under California Code of Civil Procedure § 410.10. The aggregated amount of damages incurred by Plaintiffs and the Class exceeds the $25,000 jurisdictional minimum of this Court. The amount in controversy as to the Plaintiffs individually and each individual Class member does not exceed $75,000, including interest and any pro rata award of attorneys' fees, costs, and damages. Venue is proper in this Court under California Bus. & Prof. Code § 17203, Code of Civil Procedure §§ 395(a) and 395.5 because Defendant is registered and does business in the State of California and in the County of Alameda. Defendant has obtained medical information in the transaction of business in the County of Alameda, which has caused both obligations and liability of Defendant to arise in the County of Alameda.

III.

PARTIES

A. PLAINTIFFS

8. Class Representative Plaintiff Christopher Newton is a resident of California. At all times relevant, Plaintiff was a patient of Defendant who utilized Defendant's website and web application to receive medical treatment medical treatment from Defendant, and was a patient, as defined by Civil Code § 56.05(k). Plaintiff's individual identifiable medical information derived by Defendant in electronic form was in possession of Defendant, including but not limited to Plaintiff's medical history, mental or physical condition, or treatment, including diagnosis and treatment dates.

Such medical information included or contained an element of personal identifying information sufficient to allow identification of the individual, such as Plaintiff's name, date of birth, addresses, medical record number, insurance provider, electronic mail address, telephone number, or social security number, or other information that, alone or in combination with other publicly available information, reveals Plaintiff's identity.

9. Class Representative Plaintiff Christa Vital is a resident of California. At all times relevant, Plaintiff was a patient of Defendant who utilized Defendant's website and web application to receive medical treatment from Defendant, and was a patient, as defined by Civil Code § 56.05(k). Plaintiff's individual identifiable medical information derived by Defendant in electronic form was in possession of Defendant, including but not limited to Plaintiff's medical history, mental or physical condition, or treatment, including diagnosis and treatment dates. Such medical information included or contained an element of personal identifying information sufficient to allow identification of the individual, such as Plaintiff's name, date of birth, addresses, medical record number, insurance provider, electronic mail address, telephone number, or social security number, or other information that, alone or in combination with other publicly available information, reveals Plaintiff's identity. Since receiving treatment at Defendant's facilities, Plaintiff has received numerous solicitations by mail and phone from third parties at an address and number she only provided to Defendant. She has also begun receiving phone call regarding health issues she and her family have sought treatment for.

10. Class Representative Plaintiff Scott Schutza is a resident of California. At all times relevant, Plaintiff was a patient of Defendant who utilized Defendant's website and web application to receive medical treatment medical treatment from Defendant, and was a patient, as defined by Civil Code § 56.05(k). Plaintiff's individual identifiable medical information derived by Defendant in electronic form was in possession of Defendant, including but not limited to Plaintiff's medical history, mental or physical condition, or treatment, including diagnosis and treatment dates. Such medical information included or contained an element of personal identifying information sufficient to allow identification of the individual, such as Plaintiff's name, date of birth, addresses, medical record number, insurance provider, electronic mail address, telephone number, or social security

number, or other information that, alone or in combination with other publicly available information, reveals Plaintiff's identity.

11. On April 26, 2027, Plaintiffs and the Class were informed through an article on various media outlets, such as Techcrunch that their personal medical information and personal identifying information were disclosed to "third-party advertisers, including Google, Microsoft and X (formerly Twitter)."[1] This information was subsequently confirmed by Defendant in its filing with the United States Department of Health and Human Services.

B. DEFENDANT

12. Defendant Kaiser Foundation Health Plan, Inc. is a California corporation, with its principal places of business located at One Kaiser Plaza, Oakland, CA 94612. At all times relevant, Defendant is a "provider of health care" as defined by Civil Code § 56.05(m). Prior to April 2024, Defendant created, maintained, preserved, and stored Plaintiffs' and the Class members' individually identifiable medical information onto Defendant's computer network, including but not limited to Plaintiffs' and the Class members' medical history, mental or physical condition, or treatment, including diagnosis and treatment dates. Such medical information included or contained an element of personal identifying information sufficient to allow identification of the individual, such as Plaintiffs' and the Class members' names, dates of birth, addresses, medical record numbers, insurance providers, electronic mail addresses, telephone numbers, or social security numbers, or other information that, alone or in combination with other publicly available information, reveals Plaintiffs' and the Class members' identities.

C. DOE DEFENDANTS

13. The true names and capacities, whether individual, corporate, associate, or otherwise, of Defendants sued herein as DOES 1 through 100, inclusive, are currently unknown to the Plaintiffs, who therefore sue the Defendants by such fictitious names under the Code of Civil Procedure § 474. Each of the Defendants designated herein as a DOE is legally responsible in some manner for the unlawful acts referred to herein. Plaintiffs will seek leave of court and/or amend this

[1] Whittaker, Zack. "Health insurance giant Kaiser will notify millions of a data breach after sharing patients' data with advertisers," https://techcrunch.com/2024/04/25/kaiser-permanente-health-plan-millions-data-breach/ last accessed on April 26, 2024.

complaint to reflect the true names and capacities of the Defendants designated hereinafter as DOES 1 through 100 when such identities become known. Any reference made to a named Defendant by specific name or otherwise, individually or plural, is also a reference to the actions or inactions of DOES 1 through 100, inclusive.

D. AGENCY/AIDING AND ABETTING

14. At all times herein mentioned, Defendants, and each of them, were an agent or joint venturer of each of the other Defendants, and in doing the acts alleged herein, were acting with the course and scope of such agency. Each Defendant had actual and/or constructive knowledge of the acts of each of the other Defendants, and ratified, approved, joined in, acquiesced and/or authorized the wrongful acts of each co-defendant, and/or retained the benefits of said wrongful acts.

15. Defendants, and each of them, aided and abetted, encouraged and rendered substantial assistance to the other Defendants in breaching their obligations to Plaintiffs and the Class, as alleged herein. In taking action, as particularized herein, to aid and abet and substantially assist the commissions of these wrongful acts and other wrongdoings complained of, each of the Defendants acted with an awareness of his/her/its primary wrongdoing and realized that his/her/its conduct would substantially assist the accomplishment of the wrongful conduct, wrongful goals, and wrongdoing.

IV.

FACTUAL ALLEGATIONS

A. The Unauthorized Release

16. On April 26, 2027, Plaintiffs and the Class were informed through an article on Techcrunch and other medica outlets that their personal medical information and personal identifying information were disclosed to "third-party advertisers, including Google, Microsoft and X (formerly Twitter)." [2] ("Notice"). At no point had Plaintiffs and the Class provided any authorization to Defendant to release any medical records to any person on their behalf. Nor was any information sought at this time by any third party by way of a subpoena or request for documents in discovery. ("Data Breach").

[2] *Id.*

17. The reports further stated that Defendant "conducted an investigation that found "certain online technologies, previously installed on its websites and mobile applications, may have transmitted personal information to third-party vendors.""

18. The reports also mentioned "that the data shared with advertisers includes member names and IP addresses, as well as information that could indicate if members were signed into a Kaiser Permanente account or service and how members "interacted with and navigated through the website and mobile applications, and search terms used in the health encyclopedia.""

19. According to the media reports, Defendant "subsequently removed the tracking code from its websites and mobile apps."

20. Although the reports mentioned that Defendant "filed a legally required notice with the U.S. government on April 12 but made public on Thursday confirming that 13.4 million residents had information exposed," and "notified California's attorney general of the data breach," Defendant's spokesperson confirmed that Defendant has yet to notify the affected individuals. The Notice stated "that the organization would begin notifying 13.4 million affected current and former members and patients who accessed its websites and mobile apps. The notifications will start in May in all markets where Kaiser Permanente operates, the spokesperson said."

21. As such, Plaintiffs are informed and believe that Defendant regularly gave unrestricted access to third parties to the Personal and Medical Information of Plaintiffs and all Class Members for an undetermined period of time prior to April 2024.

22. Yet, despite knowing many patients were in danger, Defendant did nothing to warn Class Members. During this time, unauthorized third parties had free reign to surveil and defraud their unsuspecting victims. Defendant proceeded business as usual without giving class members the information they needed to protect themselves against fraud and identity theft.

23. It is apparent from the reports and subsequent filings with the United States Department of Health and Human Services and the California Attorney General's office, that Defendant stores the personal medical information of the Class Members and released them to unauthorized third parties.

24. Defendant failed to adequately safeguard Plaintiffs and Class Members' Personal and Medical Information, allowing unauthorized third parties to access this wealth of priceless information for an undetermined period of time prior to April 2024, and possibly continuing to date, without warning the victims, the Class Members, to be on the lookout.

25. Defendant failed to spend sufficient resources on making sure that its patients' personal medical information are secure and released only to authorized persons.

26. Defendant had obligations created by the Health Insurance Portability and Accountability Act ("HIPAA"), the Confidentiality of Medical Information Act ("CMIA"), reasonable industry standards, its own contracts with its patients and employees, common law, and its representations to Plaintiffs and Class members, to keep their Personal and Medical Information confidential and to protect the information from unauthorized access.

27. Plaintiffs and Class members provided their Personal and Medical Information to Defendant with the reasonable expectation and mutual understanding that it would comply with its obligations to keep such information confidential and secure from unauthorized access.

28. Indeed, as discussed below, Defendant promised Plaintiffs and Class members that it would do just that.

B. Defendant Expressly Promised to Protect Personal and Medical Information

29. Defendant provides all patients, including Plaintiffs and Class members, its Notice of Privacy Practices, which states that:

> II. ABOUT OUR RESPONSIBILITY TO PROTECTYOUR PHI
>
> By law, we must
>
> 1. protect the privacy of your PHI;
> 2. tell you about your rights and our legal duties with respect to your PHI;
> 3. notify you if there is a breach of your unsecured PHI; and
> 4. tell you about our privacy practices and follow our notice currently in effect.
>
> We take these responsibilities seriously and, have put in place administrative safeguards(such as security awareness training and policies and procedures), technical safeguards(such as encryption and passwords), and physical safeguards

(such as locked areas and requiring badges) to protect your PHI and, as in the past, we will continue to take appropriate steps to safeguard the privacy of your PHI.[3]

30. Likewise, Defendant's Notice of Privacy Practices also states that:

VI. ALL OTHER USES AND DISCLOSURES OFYOUR PHI REQUIRE YOUR PRIOR WRITTENAUTHORIZATION

Except for those uses and disclosures described above, we will not use or disclose your PHI without your written authorization. Some instances in which we may request your authorization for use or disclosure of PHI are:

Marketing:
We may ask for your authorization in order to provide information about products and services that you may be interested in purchasing or using. Note that marketing communications do not include our contacting you with information about treatment alternatives, prescription drugs you are taking or health-related products or services that we offer or that are available only to our health plan enrollees. Marketing also does not include any face-to-face discussions you may have with your providers about products or services.

Sale of PHI:
We may only sell your PHI if we received your prior written authorization to do so.

Psychotherapy Notes:
On rare occasions, we may ask for your authorization to use and disclose "psychotherapy notes". Federal privacy law defines "psychotherapy notes" very specifically to mean notes made by a mental health professional recording conversations during private or group counseling sessions that are maintained separately from the rest of your medical record. Generally, we do not maintain psychotherapy notes, as defined by federal privacy law.

When your authorization is required and you authorize us to use or disclose your PHI for some purpose, you may revoke that authorization by notifying us in writing at any time. Please note that the revocation will not apply to any authorized use or disclosure of your PHI that took place before we received your revocation. Also, if you gave your authorization to secure a policy of insurance, including health care

[3] Kaiser, "Notice of Privacy Practices," Effective Date: September 22, 2023, https://healthy.kaiserpermanente.org/southern-california/privacy-practices , last visited on April 26, 2024.

> coverage from us, you may not be permitted to revoke it until the insurer can no longer contest the policy issued to you or a claim under the policy.[4]

31. Notwithstanding the foregoing assurances and promises, Defendant failed to protect the Personal and Medical Information of Plaintiffs and other Class members from releasing their information to unauthorized third parties, as conceded by Defendant in the Notice.

32. If Defendant truly understood the importance of safeguarding patients' Personal and Medical Information, it would acknowledge its responsibility for the harm it has caused, and would compensate class members, provide long-term protection for Plaintiffs and the Class, agree to Court-ordered and enforceable changes to its policies and procedures, and adopt regular and intensive training to ensure that an unauthorized release like this never happens again.

33. That information is now in the hands unauthorized third parties who will use it if given the chance. In fact, Plaintiff Vital already has begun receiving direct solicitations and advertisements from third parties regarding medical conditions she sought treatment for. Much of this information is unchangeable and loss of control of this information is remarkably dangerous to consumers.

C. Defendant had an Obligation to Protect Personal and Medical Information under Federal and State Law and the Applicable Standard of Care

34. Defendant is an entity 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.

35. HIPAA's Privacy Rule or *Standards for Privacy of Individually Identifiable Health Information* establishes national standards for the protection of health information.

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

---

[4] *Id.*

37. 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.

38. "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.

39. 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 its workforce.

40. HIPAA also required 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).

41. HIPAA also required 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).

42. Defendant was also prohibited by the Federal Trade Commission Act ("FTC Act") (15 U.S.C. §45) from engaging in "unfair or deceptive acts or practices in or affecting commerce." The Federal Trade Commission ("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).

43. In addition to their obligations under federal and state laws, Defendant owed a duty to Class Members whose Personal and Medical Information was entrusted to Defendant to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the Personal and Medical Information in its possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons. Defendant owed a duty to Class Members to provide reasonable security, including consistency with industry standards and requirements, and to ensure that its systems, policies, procedures, and the personnel responsible for them, adequately protected the Personal and Medical Information of the Class Members.

44. Defendant owed a duty to Class Members whose Personal and Medical Information was entrusted to Defendant to design, maintain, and test its systems, policies, and procedures to ensure that the Personal and Medical Information in Defendant's possession was adequately secured and protected.

45. Defendant owed a duty to Class Members whose Personal and Medical Information was entrusted to Defendant to create and implement reasonable data security practices and procedures to protect the Personal and Medical Information in their possession, including adequately training its employees and others who accessed Personal Information within its computer systems on how to adequately protect Personal and Medical Information.

46. Defendant owed a duty to Class Members whose Personal and Medical Information was entrusted to Defendant to implement processes that would detect an unauthorized access in a timely manner.

47. Defendant owed a duty to Class Members whose Personal and Medical Information was entrusted to Defendant to act upon data security warnings and alerts in a timely fashion.

48. Defendant owed a duty to Class Members whose Personal and Medical Information was entrusted to Defendant to adequately train and supervise its employees to identify and avoid any phishing emails that make it past its email filtering service.

49. Defendant owed a duty to Class Members whose Personal and Medical Information was entrusted to Defendant to disclose if its computer systems and data security practices were inadequate to safeguard individuals' Personal and Medical Information from theft or access by

unauthorized third parties because such an inadequacy would be a material fact in the decision to entrust Personal and Medical Information with Defendant.

50. Defendant owed a duty to Class Members whose Personal and Medical Information was entrusted to Defendant to disclose in a timely and accurate manner when an unauthorized access occurred.

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

D. An Unauthorized Release like this Results in Debilitating Losses to Consumers

52. Each year, identity theft causes tens of billions of dollars of losses to victims in the United States.[5] Unauthorized third parties can leverage Plaintiffs' and Class members' Personal and Medical Information that was obtained in the unauthorized release to commit thousands-indeed, millions-of additional crimes, including opening new financial accounts in Class Members' names, taking out loans in Class Members' names, using Class Members' names to obtain medical services and government benefits, using Class Members' Personal Information to file fraudulent tax returns, using Class Members' health insurance information to rack up massive medical debts in their names, using Class Members' health information to target them in other phishing and hacking intrusions based on their individual health needs, using Class Members' information to obtain government benefits, filing fraudulent tax returns using Class Members' information, obtaining driver's licenses in Class Members' names but with another person's photograph, and giving false information to police during an arrest. Even worse, Class Members could be arrested for crimes identity thieves have committed.

53. Personal and Medical Information is such a valuable commodity to identity thieves that once the information has been compromised, criminals often trade the information on the cyber black-market for years.

[5] "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").

54. This is not just speculative. As the FTC has reported, if unauthorized third parties get access to Personal and Medical Information, they ***will*** use it.[6]

55. Unauthorized third parties may not use the 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.[7]

56. Medical 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."[8]

57. "Medical identity theft is a growing and dangerous crime that leaves its victims with little to no recourse for recovery," reported Pam Dixon, executive director of World Privacy Forum. "Victims often experience financial repercussions and worse yet, they frequently discover erroneous information has been added to their personal medical files due to the thief's activities."[9]

58. As indicated by Jim 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 financial information all in one place. Credit cards can be, say, five dollars or more where PHI can go from $20 say up to—we've seen $60 or $70

---

[6] 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.

[7] *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 (emphasis added).

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

[9] *Id.*

[(referring to prices on dark web marketplaces)]."[10] A complete identity theft kit that includes health insurance credentials may be worth up to $1,000 on the black market.[11]

59. As a direct and proximate result of the unauthorized release, Plaintiffs and the Class have been placed at an imminent, immediate, and continuing increased risk of harm from fraud and identity theft. Plaintiffs and the Class must now take the time and effort to mitigate the actual and potential impact of the unauthorized release on their everyday lives, including placing "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.

60. Plaintiffs 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 and Medical Information;

b. Improper disclosure of their Personal and Medical Information;

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

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

e. Damages flowing from Defendant's untimely and inadequate notification of the unauthorized release;

f. Loss of privacy suffered as a result of the unauthorized release, including the harm of knowing unauthorized third parties have their Personal and Medical Information and that

---

[10] ID Experts, *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

[11] *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

fraudsters have already used that information to initiate spam calls to members of the Class;

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 unauthorized release;

h. Ascertainable losses in the form of deprivation of the value of customers' 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 and Medical Information; and

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

61. Moreover, Plaintiffs and Class have an interest in ensuring that their information, which remains in the possession of Defendant, is protected from further unauthorized release by the implementation of security measures and safeguards.

62. Even if Defendant would acknowledge the harm caused by the unauthorized release by recommending that Plaintiffs and Class Members review the statements they receive from their healthcare providers and health insurer, any amount of identity theft repair and monitoring is woefully inadequate to protect Plaintiffs and Class members from a lifetime of identity theft risk and worse, it does nothing to reimburse Plaintiffs and Class members for the injuries they have already suffered.

V.

CLASS ACTION ALLEGATIONS

63. Class Representative Plaintiffs bring this action on their own behalf and on behalf of all other persons similarly situated. The putative class that Class Representative Plaintiffs seek to represent is composed of:

> All patients of Defendant who received treatment at one of Defendant's hospital, satellite, or urgent care locations and whose personal medical information were released to third parties without authorization (hereinafter the "Class").

Excluded from the Class are the natural persons who are directors, and officers, of the Defendant, as well as Plaintiffs' counsel, judges, clerks, and other supporting staff of the Superior Court of California by and for the County of Alameda. Class Representative Plaintiffs expressly disclaims that he is seeking a class-wide recovery for personal injuries attributable to Defendant's conduct.

64. Plaintiffs are informed and believe that the members of the Class are so numerous that joinder of all members is impracticable. While the exact number of the Class members is unknown to Class Representative Plaintiffs at this time, such information can be ascertained through appropriate discovery, from records maintained by Defendant. According to the Defendant's filings with the United States Department of Health and Human Services, 13.4 million consumers, including 9.6 million Californians, were affected by this intentional sale of confidential medical information.

65. There is a well-defined community of interest among the members of the Class because common questions of law and fact predominate, Class Representative Plaintiffs' claims are typical of the members of the class, and Class Representative Plaintiffs can fairly and adequately represent the interests of the Class.

66. Common questions of law and fact exist as to all members of the Class and predominate over any questions affecting solely individual members of the Class. Among the questions of law and fact common to the Class are:

(a) Whether Defendant failed to adequately safeguard Plaintiffs and the Class's Personal and Medical Information;

(b) Whether Defendant sold information to third party advertisers;

(c) Whether the type of information sold by Defendant to third party advertisers constitutes confidential medical information as defined by Civil Code §56.05(j);

(d) Whether Defendant failed to protect Plaintiffs and the Class's Personal and Medical Information;

(e) Whether Defendant's policy of selling data gathered from the Class on its websites and web applications violated the FTC Act, HIPAA, CMIA, and/or Defendant's other duties;

(d) Whether Defendant violated the data security statutes and notification statutes applicable to Plaintiffs and the Class;

(e) Whether Defendant failed to notify Plaintiffs and members of the Class about the unauthorized release expeditiously and without unreasonable delay after the

unauthorized release was discovered;

(f) Whether Defendant engaged in unfair, unlawful, or deceptive practices by failing to safeguard Class Members' Personal and Medical Information properly and as promised;

(g) Whether Defendant entered into implied contracts with Plaintiffs and the members of the Class that included contract terms requiring Defendant to protect the confidentiality of Personal and Medical Information and have reasonable security measures;

(h) Whether Defendant violated the consumer protection statutes and state medical privacy statutes applicable to Plaintiffs and the Class;

(i) Whether Defendant failed to notify Plaintiffs and Class Members about the unauthorized release as soon as practical and without delay after the unauthorized release was discovered;

(j) Whether Defendant's conduct described herein constitutes a breach of their implied contracts with Plaintiffs and the Class;

(k) Whether Plaintiffs and the members of the Class are entitled to damages as a result of Defendant's wrongful conduct;

(l) What equitable relief is appropriate to redress Defendant's wrongful conduct;

(m) What injunctive relief is appropriate to redress the imminent and currently ongoing harm faced by Plaintiffs and members of the Class;

(n) Whether Defendant acted negligently in failing to safeguard Plaintiffs' and the Class's Personal and Medical Information, including whether its conduct constitutes negligence; and

(o) Whether Defendant acted negligently in failing to safeguard Plaintiffs' and the Class's Personal and Medical Information, including whether its conduct constitutes negligence *per se*.

Class Representative Plaintiffs' claims are typical of those of the other Class members because Class Representative Plaintiffs, like every other Class member, were exposed to virtually identical conduct and is entitled to nominal damages of one thousand dollars ($1,000) per violation pursuant to Civil Code §§ 56.101 and 56.36(b)(1).

67. Class Representative Plaintiffs will fairly and adequately protect the interests of the Class. Moreover, Class Representative Plaintiffs have no interest that is contrary to or in conflict with those of the Class they seek to represent during the Class Period. In addition, Class Representative Plaintiffs have retained competent counsel experienced in class action litigation to further ensure such protection and intend to prosecute this action vigorously.

68. The prosecution of separate actions by individual members of the Class would create a risk of inconsistent or varying adjudications with respect to individual members of the Class, which would establish incompatible standards of conduct for the Defendant in the State of California and would lead to repetitious trials of the numerous common questions of fact and law in the State of California. Class Representative Plaintiffs know of no difficulty that will be encountered in the management of this litigation that would preclude its maintenance as a class action. As a result, a class action is superior to other available methods for the fair and efficient adjudication of this controversy.

69. Proper and sufficient notice of this action may be provided to the Class members through direct mail.

70. Moreover, the Class members' individual damages are insufficient to justify the cost of litigation, so that in the absence of class treatment, Defendant's violations of law inflicting substantial damages in the aggregate would go unremedied without certification of the Class. Absent certification of this action as a class action, Class Representative Plaintiffs and the members of the Class will continue to be damaged by the unauthorized release of their individual identifiable medical information.

VI.

CAUSES OF ACTION

FIRST CAUSE OF ACTION

(Violations of the Confidentiality of Medical Information Act, Civil Code § 56, *et seq.*)

(Against All Defendants)

71. Plaintiffs and the Class incorporate by reference all of the above paragraphs of this Complaint as though fully stated herein.

72. Defendant is a "provider of health care," within the meaning of Civil Code § 56.05(m), and maintained and continues to maintain "medical information," within the meaning of Civil Code § 56.05(j), of "patients" of the Defendant, within the meaning of Civil Code § 56.05(k).

73. Plaintiffs and the Class are "patients" of Defendant within the meaning of Civil Code § 56.05(k). Furthermore, Plaintiffs and the Class, as patients of Defendant, had their individually identifiable "medical information," within the meaning of Civil Code § 56.05(j), stored onto

Defendant's server, and received treatment at one of Defendant's hospital, satellite, or urgent care locations on or before April 2024. Plaintiffs and the Class also utilized Defendant's website and/or web application to research medical conditions, make appointments with their physicians for specific medical conditions, email their physicians regarding medical questions they had, amongst other medical uses.

74. On April 26, 2027, Plaintiffs and the Class were informed through an article on Techcrunch, along with other media outlets that Defendant released to "third-party advertisers, including Google, Microsoft and X (formerly Twitter)" Plaintiffs' and the Class's individual identifiable "medical information," within the meaning of Civil Code § 56.05(j),[12] including "member names and IP addresses, as well as information that could indicate if members were signed into a Kaiser Permanente account or service and how members "interacted with and navigated through the website and mobile applications, and search terms used in the health encyclopedia." [13]

75. Despite realizing the unauthorized release of Plaintiffs' personal medical information, Defendant has yet to inform Plaintiffs and the Class Members about the approximate duration of the issue in its policies and procedures that allowed unauthorized individual(s) access to Plaintiffs' and the Class Members' personal medical information.

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

77. Because Civil Code § 56.101 allows for the remedies and penalties provided under Civil Code § 56.36(b), Plaintiffs individually and on behalf of the Class seek nominal damages of

---

[12] Pursuant to Civil Code § 56.05(j), "Medical information" means "any individually identifiable information, in electronic or physical form, in possession of or derived from a provider of health care...regarding a patient's medical history, mental or physical condition, or treatment. 'Individually Identifiable' means that the medical information includes or contains any elements of personal identifying information sufficient to allow identification of the individual, such as the patient's name, address, electronic mail address, telephone number, or social security number, or other information that, alone or in combination with other publicly available information, reveals the individual's identity."

[13] Whittaker, Zack. "Health insurance giant Kaiser will notify millions of a data breach after sharing patients' data with advertisers," https://techcrunch.com/2024/04/25/kaiser-permanente-health-plan-millions-data-breach/ last accessed on April 26, 2024.

one thousand dollars ($1,000) for each violation under Civil Code § 56.36(b)(1); and Plaintiffs individually seek actual damages suffered, if any, pursuant to Civil Code § 56.36(b)(2).

SECOND CAUSE OF ACTION
(Violations of the CALIFORNIA UNFAIR COMPETITION LAW, Cal. Bus. & Prof. Code §17200, *et seq.*)

78. Plaintiffs incorporate by reference all allegations of the preceding paragraphs as though fully set forth herein.

79. Defendant is organized under the laws of California. 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 their Personal and Medical Information from unauthorized disclosure, release, data breach, and theft; representing and advertising that they did and would comply with the requirement of relevant federal and state laws pertaining to the privacy and security of the Class' Personal and Medical Information; and omitting, suppressing, and concealing the material fact of the inadequacy of the privacy and security protections for the Class' Personal and Medical Information;

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

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

d. by violating the CMIA, Cal. Civ. Code § 56, *et seq.*

80. These unfair acts and practices were immoral, unethical, oppressive, unscrupulous, unconscionable, and/or substantially injurious to Plaintiffs and Class members. Defendant's practice was also contrary to legislatively declared and public policies that seek to protect consumer data and ensure that entities who 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 CMIA, Cal. Civ. Code § 56, *et seq.*

81. As a direct and proximate result of Defendant's unfair and unlawful practices and acts, Plaintiffs 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 and Medical Information, and additional losses described above. In addition, Defendant treated the personal and medical information of Plaintiffs and the Class as its own property, and sold it for profit, causing a loss of money and property to Plaintiffs and the Class.

82. Defendant knew or should have known that its sale of information to third party advertisers would violate the CMIA, HIPAA and the FTC, and would fail to safeguard Plaintiffs and Class members' Personal and Medical Information. Defendant's actions in engaging in the above-named unfair practices and deceptive acts were intentional, knowing and willful, and/or wanton and reckless with respect to the rights of the Class.

83. The conduct and practices described above emanated from California where decisions related to Defendant's advertising and data security were made.

84. Plaintiffs seek relief under the UCL, including restitution to the Class of money or property that the Defendant may have acquired, including all monies it received through the sale of this medical information, 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.

THIRD CAUSE OF ACTION
(NEGLIGENCE)

85. Plaintiffs incorporate by reference all allegations of the preceding paragraphs as though fully set forth herein.

86. Defendant required Plaintiffs and Class Members to submit non-public, sensitive PII and other data via its contracts with the respective health care providers.

87. Defendant had, and continues to have, a duty to Plaintiffs and Class Members to exercise reasonable care in safeguarding and protecting their Private Information and other data. Defendant also had, and continues to have, a duty to use ordinary care in activities from which harm might be reasonably anticipated, such as in the collection, storage and protection of Private Information and other data within their possession, custody and control and that of its vendors.

88. Defendant's duty to use reasonable security measures arose as a result of the special relationship that existed between Defendant and patients and former patients. The special relationship arose because Plaintiffs and the Members of the Class had entrusted Defendant with their Private Information and other data by virtue of being patients at the respective health care providers with which Defendant had contracted to provide services. Only Defendant was in a position to ensure that its systems were sufficient to protect against the harm to Plaintiffs and the Class Members from a data breach.

89. Defendant violated these standards and duties by failing to exercise reasonable care in safeguarding and protecting Plaintiffs and Class Members' Private Information and other data by failing to design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems to safeguard and protect the Private Information and other data entrusted to it, including Plaintiffs' and Class Members' Private Information and other data as aforesaid. It was reasonably foreseeable to Defendant that its failure to exercise reasonable care in safeguarding and protecting Plaintiffs' and Class Members' Private Information and other data by failing to design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems would result in the unauthorized release, disclosure, and dissemination of Plaintiffs' and Class Members' Private Information and other data.

90. Defendant, by and through its negligent actions, inaction, omissions, and want of ordinary care, unlawfully breached its duties to Plaintiffs and Class Members by, inter alia, failing

to exercise reasonable care in safeguarding and protecting Plaintiffs and Class Members' Private Information and other data within their possession, custody and control.

91. Defendant, by and through its negligent actions, inactions, omissions, and want of ordinary care, further breached its duties to Plaintiffs and Class Members by failing to design, adopt, implement, control, direct, oversee, manage, monitor and audit their processes, controls, policies, procedures, protocols, and software and hardware systems for complying with the applicable laws and safeguarding and protecting their Private Information and other data.

92. But for Defendant's negligent breach of the above-described duties owed to Plaintiffs and Class Members, their Private Information and other data would not have been released, disclosed, and disseminated without their authorization.

93. Plaintiffs' and Class Members' Private Information and other data was transferred, sold, opened, viewed, mined and otherwise released, disclosed, and disseminated to unauthorized persons without their authorization as the direct and proximate result of Defendant's failure to design, adopt, implement, control, direct, oversee, manage, monitor and audit its processes, controls, policies, procedures and protocols for complying with the applicable laws and safeguarding and protecting Plaintiffs' and Class Members' Private Information and other data.

94. As a direct and proximate result of Defendant's above-described wrongful actions, inaction, omissions, and want of ordinary care that directly and proximately caused the Data Breach, Plaintiffs and Class Members have suffered, and will continue to suffer, ongoing, imminent, and impending threat of identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; loss of the confidentiality of the stolen confidential data; the illegal sale of the compromised data on the dark web; expenses and/or time spent on credit monitoring and identity theft insurance; time spent scrutinizing bank statements, credit card statements, and credit reports; expenses and/or time spent initiating fraud alerts, decreased credit scores and ratings; lost work time; and other economic and noneconomic harm.

95. Defendant's above-described wrongful actions, inaction, omissions, and want of ordinary care that directly and proximately caused this Data Breach constitute negligence.

96. Plaintiffs are entitled to compensatory and consequential damages suffered as a result of the Data Breach.

97. Plaintiffs are also entitled to injunctive relief requiring Defendant to, e.g., (i) strengthen its data security programs and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) immediately provide robust and adequate credit monitoring to all Class Members, and any other relief this Court deems just and proper.

FOURTH CAUSE OF ACTION
(NEGLIGENCE PER SE)

98. Plaintiffs incorporate by reference all allegations of the preceding paragraphs as though fully set forth herein.

99. Pursuant to the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45, Defendant had a duty to provide fair and adequate computer systems and data security to safeguard the personal and financial information of Plaintiffs and Class Members.

100. The FTCA 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 the Private Information and other data of Plaintiffs and Class Members. The pertinent FTC publications and orders form part of the basis of Defendant's duty in this regard.

101. Defendant required, gathered, and stored personal and financial information of Plaintiffs and Class Members to fulfill its contracts with the various and several health care providers.

102. Defendant violated the FTCA by failing to use reasonable measures to protect the Private Information and other data of Plaintiffs and Class Members and by not complying with applicable industry standards, as described herein.

103. Plaintiffs and Class Members are within the class of persons that the FTC Act was intended to protect.

104. The harm that occurred as a result of the Data Breach is the type of harm the FTCA was intended to guard against. The FTC has pursued enforcement actions against businesses,

which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiffs and Class Members.

105. As a direct and proximate result of Defendant's negligence per se, Plaintiffs and Class Members have suffered, and continue to suffer, injuries, damages arising from identify theft; from their needing to contact agencies administering unemployment benefits; potentially defending themselves from legal action base upon fraudulent applications for unemployment benefits made in their name; contacting their financial institutions; loss of use of funds; closing or modifying financial accounts; damages from lost time and effort to mitigate the actual and potential impact of the data breach on their lives; closely reviewing and monitoring their accounts for unauthorized activity which is certainly impending; placing credit freezes and credit alerts with credit reporting agencies; and damages from identify theft, which may take months or years to discover and detect.

106. Defendant's violation of the FTCA constitutes negligence per se.

107. For the same reasons and upon the same bases, Defendant's violation of the CMIA, UCL, and various other State and local statutes, constitutes negligence per se.

108. As a direct and proximate result of Defendant's violation of the foregoing statutes and regulations, Plaintiffs and Class Members have suffered injury and are entitled to compensatory, consequential, and punitive damages in an amount to be proven at trial.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs respectfully request the Court to grant Plaintiffs and the Class members the following relief against Defendant:

a. An order certifying this action as a class action under Code of Civil Procedure §382, defining the Class as requested herein, appointing the undersigned as Class counsel, and finding that Plaintiffs are proper representatives of the Class requested herein;

b. A judgment in favor of Plaintiffs and the Class awarding them appropriate monetary relief, including actual and statutory damages, including statutory damages under the CMIA,

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 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 their security personnel regarding any new or modified procedures;

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

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

vii. Ordering that Defendant routinely and continually conduct internal training and education to inform internal security personnel how to identify and contain an unauthorized release when it occurs and what to do in response to an unauthorized release; and

viii. Ordering Defendant to meaningfully educate its current, former, and prospective employees and subcontractors about the threats they face as a

result of the loss of their financial and personal information to third parties, as well as the steps they must take to protect themselves.;

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

e. Restitutionary disgorgement of all wrongly acquired monies received by Defendant from the sale of the medical information of Plaintiffs and the Class Members, including monies directly received from advertisers;

f. A judgment in favor of Plaintiffs and the Class awarding them pre-judgment and post-judgment interest, reasonable attorneys' fees, costs and expenses as allowable by law, including the UCL, Cal. Bus. & Prof. Code § 17082 and the CMIA, Cal. Civ. Code 56.35; and

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

POTTER HANDY LLP

Dated: April 29, 2024 By: /s/ James M. Treglio
Mark D. Potter, Esq.
James M. Treglio, Esq.
Attorneys for the Plaintiffs and the Class

DEMAND FOR JURY TRIAL

Plaintiffs and the Class hereby demand a jury trial on all causes of action and claims with respect to which they have a right to jury trial.

POTTER HANDY LLP

Dated: April 29, 2024 By: /s/ James M. Treglio
Mark D. Potter, Esq.
James M. Treglio, Esq.
Attorneys for the Plaintiffs and the Class