Tina Wolfson, California Bar No. 174806
AHDOOT & WOLFSON, PC
10728 Lindbrook Drive
Los Angeles, CA 90024
Tel: (310) 474-9111
Fax: (310) 474-8585
twolfson@ahdootwolfson.com

Cornelius P. Dukelow, Oklahoma Bar No. 19086
ABINGTON COLE + ELLERY
320 South Boston Avenue
Suite 1130
Tulsa, Oklahoma 74103
918.588.3400 (*telephone & facsimile*)
cdukelow@abingtonlaw.com

Benjamin F. Johns, Pennsylvania Bar No. 201373
Andrew W. Ferich, Pennsylvania Bar No. 313696
CHIMICLES SCHWARTZ KRINER & DONALDSON-SMITH LLP
One Haverford Centre
361 Lancaster Avenue
Haverford, Pennsylvania 19041
610.642.8500
bfj@chimicles.com
awf@chimicles.com

Attorneys for Plaintiffs and the Proposed Classes

UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF CALIFORNIA

VICKI STASI, SHANE WHITE, and CRYSTAL GARCIA, individually and on behalf of all others similarly situated,

Plaintiffs,

v.

INMEDIATA HEALTH GROUP CORP.; and DOES 1 through 20, inclusive,

Defendants.

Case No. 19-cv-02353-JM-LL

FIRST AMENDED CLASS ACTION COMPLAINT

DEMAND FOR JURY TRIAL

Plaintiffs, Vicki Stasi, Shane White, and Crystal Garcia ("Plaintiffs"), on behalf of themselves individually and on behalf of all others similarly situated, allege on personal knowledge, investigation of counsel, and on information and belief as follows:

BRIEF SUMMARY OF THE CASE

1. This case comes as a result of Inmediata, a third party service provider, posting highly sensitive personal and medical information of over half a million patients on the internet.

2. In January of 2019, Inmediata Health Group Corp. ("Inmediata" or "Defendant") first learned that it was experiencing a large data breach (hereinafter "Data Breach") that resulted in the unauthorized acquisition, access, use, or disclosure of unsecured protected health information and personal information of approximately 1,565,338 individuals (hereinafter "Class Members"), including Plaintiffs. As a result of the Data Breach, the security and privacy of Plaintiffs' and Class Members' protected health information and personal information was compromised.

3. After investigating the Data Breach, Inmediata filed a breach report with the Secretary of the U.S. Department of Health and Human Services pursuant to 45 CFR § 164.408(a) (hereinafter "Breach Report").

4. In addition to revealing that 1,565,338 individuals were affected by the Data Breach, the Breach Report characterizes the Data Breach as an "unauthorized access/disclosure" of unsecured protected health information and further indicates that the breached unsecured protected health information was located on a "network server".

5. Plaintiffs' and Class Members' unsecured protected health information and personal information compromised in the Data Breach as a direct result of Inmediata's acts and/or omissions included the types of information that people consider extremely sensitive and private and the types of information that federal and state law require companies to take security measures to protect: names, addresses, Social Security numbers, dates of birth, gender, and medical claim information including dates of service, diagnosis codes, procedure codes and treating physicians (hereinafter "Personal and

Medical Information"). This extremely sensitive data should have received the most rigorous protection available – it did not.

6. Inmediata was storing Plaintiffs' and Class Members' sensitive and confidential Personal and Medical Information, which it knew Class Members consider extremely private, and which is valuable to criminals and vulnerable to exfiltration. Inmediata failed to take security precautions necessary to protect the Personal and Medical Information.

7. In short, Inmediata posted on the Internet Plaintiffs' and Class Members' Personal and Medical Information. Due to a webpage setting that permitted search engines to index webpages Inmediata uses for business operations, Plaintiffs' and Class Members' Personal and Medical Information was also searchable and findable by anyone with access to an internet search engine such as Google, Yahoo, Bing, etc.

8. Because Inmediata failed to take basic, elementary, and necessary security precautions, Plaintiffs' and Class Members' Personal and Medical Information was disclosed and released to the entire world – it was viewable online by anyone in the world, printable by anyone in the world, copiable by anyone in the world, and downloadable by anyone in the world.

9. It didn't take a thief or a hacker to exploit Inmediata's lax security, exfiltrate the information, and then post the information on a criminal underworld website; Inmediata skipped the intermediary and – on its own! – posted on the Internet Plaintiffs' and Class Members' Personal and Medical Information.

PARTIES

10. Plaintiff Vicki Stasi is an individual residing in Seminole, Florida.

11. Plaintiff Shane White is an individual residing in Moorhead, Minnesota.

12. Plaintiff Crystal Garcia is an individual residing in Poway, California.

13. Defendant Inmediata Health Group Corp. is a Puerto Rico corporation with its principal place of business and headquarters in San Juan, Puerto Rico.

JURISDICTION AND VENUE

14. This Court has subject matter jurisdiction over this matter pursuant to 28 U.S.C. § 1332(d) because the amount in controversy exceeds $5,000,000 (exclusive of interests and costs), because there are more than 100 members in each of the proposed classes, and because at least one member of each of the proposed classes is a citizen of a State different from Defendant.

15. This Court has personal jurisdiction over Defendant because it regularly conducts business in California.

16. Venue is proper in this Court pursuant to 28 U.S.C. § 1391 because a substantial part of the events, acts, and omissions giving rise to Plaintiffs' claims occurred in, was directed to, and/or emanated from this District.

STATEMENT OF FACTS

Defendant

17. Inmediata is a Health Care Clearinghouse as defined by 42 U.S.C. § 1320d and provides a variety of software and service solutions to healthcare providers.

18. Inmediata's service solutions include SecureValue, SecureAlly, and SecureAR. SecureValue is an aggregator of clinical and financial data for patients from a variety of sources, including claim, electronic health record, lab, pharmacy, hospital and other data sources. SecureAlly is a cloud-based business process outsourcing solution for claims adjudication. SecureAR is an accounts receivable solution.

19. Inmediata's software solutions include SecureTrack and SecureClaim. SecureTrack is a full featured clearinghouse solution that integrates with practice management systems and electronic health record solutions. SecureTrack supports multiple specialty types including medical, dental, allied health, ambulance, and hospitals. SecureTrack supports billing for professional, dental, and institutional claims. SecureClaim is a practice management solution that integrates with clearinghouse and electronic health record solutions. SecureClaim supports multiple specialty types

including medical, dental, allied health and ambulance. SecureClaim supports billing for professional, dental, and institutional claims.

The Data Breach

20. On or about April 24, 2019, Inmediata publicly admitted via a press release that: "In January 2019, Inmediata became aware that some electronic health information was viewable online due to a webpage setting that permitted search engines to index internal webpages that are used for business operations." Inmediata's press release is attached hereto as **Exhibit 1**.

21. Neither the press release nor any of the other Data Breach notices or Breach Reports indicate when the Data Breach began.

22. The Data Breach resulted in the unauthorized acquisition, access, use, or disclosure of unsecured protected health information and personal information of Plaintiffs and Class Members.

23. As a result of the Data Breach, the security and privacy of Plaintiffs' and Class Members' protected health information and personal information was compromised.

24. Although Inmediata knew of the Data Breach no later than January of 2019, Inmediata took no steps to notify patients whose information was affected until April 22, 2019, when Inmediata began mailing notification letters to the potentially affected individuals directly and until April 24, 2019, via a post on Inmediata's website.

25. Although Inmediata knew of the Data Breach no later than January 31, 2019, (and likely earlier) Inmediata took no steps to directly notify Plaintiffs and Class Members until no earlier than April 22, 2019, when Defendant began mailing data breach notification letters to Plaintiffs and Class Members. This was a delay of not less than 81 days.

The California Attorney General Notice

26. On or about April 22, 2019, Inmediata began filing with various state Attorneys General (including California) sample "Notice of Data Security Incident"

letters that mirrored the language of letters Inmediata sent to Plaintiffs and Class Members. The California Notice of Data Security Incident sample letters are attached hereto as **Exhibit 2**.[1]

27. The Notice of Data Security Incident explained that "[i]n January 2019, Inmediata became aware that some of its member patients' electronic patient health information was publicly available online as a result of a webpage setting that permitted search engines to index pages that are part of an internal website we use for our business operations."

28. The Notice of Data Security Incident (non-SSN version) stated that "information potentially impacted by this incident may have included your name, address, date of birth, gender, and medical claim information including dates of service, diagnosis codes, procedure codes and treating physician."

29. The Notice of Data Security Incident (SSN version) stated that "information potentially impacted by this incident may have included your name, address, Social Security number, date of birth, gender, and medical claim information including dates of service, diagnosis codes, procedure codes and treating physician."

30. Both versions of the Notice of Data Security Incident claim that financial information was not involved. As explained below, Plaintiffs do not accept this as an accurate statement. It is a self-serving statement that has not been subjected to independent verification and Plaintiffs are under no obligation to take it at face value. Furthermore, Inmediata's own Notice of Data Security Incident advises recipients to: "review[] your account statements regularly and credit reports closely" and to "keep[] a

---

[1] Two versions of the sample letters were filed with the California Attorney General – one for victims whose Social Security Numbers *were* purportedly part of the Data Breach, and one for victims whose Social Security Numbers *were not* purportedly part of the Data Breach. Each of the Plaintiffs herein received the version of the two notices for victims whose Social Security Numbers *were not* purportedly part of the Data Breach.

close eye on your credit card activity".[2] If financial information was not involved, this advice would not have made sense. Finally, companies experiencing data breaches have often, upon further investigation after the initiation of litigation, been found to have misreported the kind of data involved in the data breach, or reported that certain information was not involved in the data breach, when in fact it was.

31. Irrespective of whether or not payment information is involved, the unauthorized disclosure of medical information can lead to medical fraud, the ramifications of which can be profound. https://www.consumer.ftc.gov/articles/0171-medical-identity-theft. A thief of medical information can use a Class Member's name or health insurance numbers to see a doctor, get prescription drugs, file claims with the patient's insurance provider, or get other care. If the thief's health information is mixed with that of a Class Member, a Class Member's treatment, then insurance records, payment records, and credit histories may be affected.

32. Inmediata's Notice of Data Security Incident acknowledged the very real threat that the incident would result in identity theft, fraud, and other similar risks by further informing recipients of the notice—Plaintiffs and Class Members—to "remain vigilant by reviewing your account statements and credit reports closely."

33. Inmediata's Notice of Data Security Incident also instructed victims to "promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, your state attorney general, and/or the Federal Trade Commission (FTC)."

34. Notably, Inmediata did not and has not, to date, offered or provided any fraud insurance or identity monitoring services to victims of the Data Breach whose Social Security Numbers were not, according to Inmediata, affected. Instead, Inmediata merely provided these victims with contact information for Experian, Transunion, and

[2] *See* Exhibit 2.

Equifax as well as for the Federal Trade Commission-Consumer Response Center. Inmediata made general suggestions to contact local authorities and police, in addition to suggestions on implementing a credit freeze if necessary. Inmediata failed to make any additional effort to mitigate or remediate the damage caused by its failure to protect sensitive personal and medical information.

35. Inmediata's own statements confirm that the Plaintiffs and the Class Members are subject to continued, future risk of identity theft, fraudulent charges and other damages. For instance, Inmediata warned consumers "remain vigilant by reviewing your account statements and credit reports closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. You also should promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, your state attorney general, and/or the Federal Trade Commission (FTC)."

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

37. 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."

38. Plaintiffs' and Class Members' Personal and Medical Information is "personal information" as defined by California Civ. Code § 1798.82(h).

39. 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".

40. 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."

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

42. Thus, Inmediata filed and disseminated these breach notifications because Plaintiffs' and Class Members' unencrypted personal information was acquired by an unauthorized person or persons as a result of the Data Breach.

43. Inmediata reasonably believes Plaintiffs' and Class Members' unencrypted personal information was acquired by an unauthorized person as a result of the Data Breach.

44. The security, confidentiality, or integrity of Plaintiffs' and Class Members' unencrypted personal information was compromised by Inmediata as a result of the Data Breach.

45. Inmediata reasonably believes the security, confidentiality, or integrity of Plaintiffs' and Class Members' unencrypted personal information was compromised by Inmediata as a result of the Data Breach.

46. Inmediata reasonably believes Plaintiffs' and Class Members' unencrypted personal information that was acquired by an unauthorized person as a result of the Data Breach, and was viewed by unauthorized persons.

47. It is reasonable to infer that Plaintiffs' and Class Members' unencrypted personal information that was acquired by an unauthorized person as a result of the Data Breach was viewed by unauthorized persons.

48. It should be rebuttably presumed that Plaintiffs' and Class Members' unencrypted personal information that was acquired by an unauthorized person as a result of the Data Breach was viewed by unauthorized persons.

49. After receiving letters sent pursuant to California Civ. Code § 1798.82(a)(1) – and filed with the Attorney General of California in accordance with California Civ. Code § 1798.82(f) – it is reasonable for recipients, including Plaintiffs and Class

Members in this case, to believe that future harm (including identity theft) is real and imminent, and to take steps to mitigate that risk of future harm.

The U.S. Department of Health and Human Services Breach Report

50. A Breach Report regarding the Data Breach filed by Inmediata with the Secretary of the U.S. Department of Health and Human Services on May 7, 2019, states that 1,565,338 individuals were affected by the Data Breach. The May 7, 2019, Breach Report characterizes the Data Breach as an "unauthorized access/disclosure" and further indicates that the breached information was located on a "network server".

51. The Breach Report filed by Inmediata on May 7, 2019, with the Secretary of the U.S. Department of Health and Human Services was filed in accordance with 45 CFR § 164.408(a).

52. Plaintiffs' and Class Members' Personal and Medical Information is "protected health information" as defined by 45 CFR § 160.103.

53. Pursuant to 45 CFR § 164.408(a), Breach Reports are filed with the Secretary of the U.S. Department of Health and Human Services "following the discovery of a breach of unsecured protected health information".

54. 45 CFR § 164.402 defines "breach" as "the acquisition, access, use, or disclosure of protected health information in a manner not permitted under subpart E of this part which compromises the security or privacy of the protected health information."

55. 45 CFR § 164.402 defines "unsecured protected health information" as "protected health information that is not rendered unusable, unreadable, or indecipherable to unauthorized persons through the use of a technology or methodology specified by the [HHS] Secretary[.]"

56. Plaintiffs' and Class Members' Personal and Medical Information is "unsecured protected health information" as defined by 45 CFR § 164.402.

57. Plaintiffs' and Class Members' unsecured protected health information has been acquired, accessed, used, or disclosed in a manner not permitted under 45 CFR Subpart E as a result of the Data Breach.

58. Inmediata reasonably believes Plaintiffs' and Class Members' unsecured protected health information has been acquired, accessed, used, or disclosed in a manner not permitted under 45 CFR Subpart E as a result of the Data Breach.

59. Plaintiffs' and Class Members' unsecured protected health information acquired, accessed, used, or disclosed in a manner not permitted under 45 CFR Subpart E as a result of the Data Breach was not rendered unusable, unreadable, or indecipherable to unauthorized persons.

60. Inmediata reasonably believes Plaintiffs' and Class Members' unsecured protected health information acquired, accessed, used, or disclosed in a manner not permitted under 45 CFR Subpart E as a result of the Data Breach was not rendered unusable, unreadable, or indecipherable to unauthorized persons.

61. Plaintiffs' and Class Members' unsecured protected health information that was acquired, accessed, used, or disclosed in a manner not permitted under 45 CFR Subpart E as a result of the Data Breach, and which was not rendered unusable, unreadable, or indecipherable to unauthorized persons, was viewed by unauthorized persons.

62. Plaintiffs' and Class Members' unsecured protected health information was viewed by unauthorized persons in a manner not permitted under 45 CFR Subpart E as a result of the Data Breach.

63. Inmediata reasonably believes Plaintiffs' and Class Members' unsecured protected health information was viewed by unauthorized persons in a manner not permitted under 45 CFR Subpart E as a result of the Data Breach.

64. It is reasonable to infer that Plaintiffs' and Class Members' unsecured protected health information that was acquired, accessed, used, or disclosed in a manner not permitted under 45 CFR Subpart E as a result of the Data Breach, and which was not rendered unusable, unreadable, or indecipherable to unauthorized persons, was viewed by unauthorized persons.

65. It should be rebuttably presumed that unsecured protected health information acquired, accessed, used, or disclosed in a manner not permitted under 45 CFR Subpart E, and which was not rendered unusable, unreadable, or indecipherable to unauthorized persons, was viewed by unauthorized persons.

66. After receiving notice that they were victims of a data breach that required the filing of a Breach Report in accordance with 45 CFR § 164.408(a), it is reasonable for recipients of that notice, including Plaintiffs and Class Members in this case, to believe that future harm (including identity theft) is real and imminent, and to take steps to mitigate that risk of future harm.

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

67. Inmediata had obligations created by HIPAA (42 U.S.C. § 1302d *et. seq.*), California's Confidentiality of Medical Information Act (Cal. Civ. Code § 56 *et seq.*), California's Consumer Records Act (Cal. Civ. Code § 1798.82 *et seq.*) and based on industry standards, to keep the compromised Personal and Medical Information confidential and to protect it from unauthorized disclosures. Plaintiffs' and Class Members' Personal and Medical Information was provided to Inmediata with the common sense understanding that Inmediata would comply with its obligations to keep such information confidential and secure from unauthorized disclosures.

68. Inmediata's data security obligations and promises were particularly important given the substantial increase in data breaches – particularly those in the healthcare industry – which were widely known to the public and to anyone in Inmediata's industries.

69. Inmediata 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.

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

71. 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 maintained or transferred in electronic form.

72. HIPAA requires Inmediata 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.

73. "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.

74. HIPAA's Security Rule requires Inmediata 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.

75. HIPAA also required Inmediata 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).

76. HIPAA also required Inmediata 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).

77. The HIPAA Breach Notification Rule, 45 CFR §§ 164.400-414, also required Inmediata to provide notice of the breach to each affected individual "without unreasonable delay and ***in no case later than 60 days following discovery of the breach***."[3]

78. Inmediata's security failures demonstrate that it failed to honor its duties and promises by not:

a. Maintaining an adequate data security system to reduce the risk of data leaks, data breaches, and cyber-attacks;

b. Adequately protecting Plaintiffs' and Class Members' Personal and Medical Information;

c. Ensuring the confidentiality and integrity of electronic protected health information it created, received, maintained, and/or transmitted, in violation of 45 C.F.R. § 164.306(a)(1);

d. Implementing 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 in violation of 45 C.F.R. § 164.312(a)(1);

e. Implementing policies and procedures to prevent, detect, contain, and correct security violations in violation of 45 C.F.R. § 164.308(a)(1)(i);

f. Implementing procedures to review records of information system activity regularly, such as audit logs, access reports, and security incident tracking reports in violation of 45 C.F.R. § 164.308(a)(1)(ii)(D);

---

[3] Breach Notification Rule, U.S. Dep't of Health & Human Services, https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html (emphasis added) (last visited May 18, 2020).

g. Protecting against any reasonably anticipated threats or hazards to the security or integrity of electronic protected health information in violation of 45 C.F.R. § 164.306(a)(2);

h. Protecting against reasonably anticipated uses or disclosures of electronic protected health information that are not permitted under the privacy rules regarding individually identifiable health information in violation of 45 C.F.R. § 164.306(a)(3);

i. Ensuring compliance with the HIPAA security standard rules by its workforce in violation of 45 C.F.R. § 164.306(a)(4); and/or

j. Training all members of its workforce effectively on the policies and procedures with respect to protected health information as necessary and appropriate for the members of its workforce to carry out their functions and to maintain security of protected health information, in violation of 45 C.F.R. § 164.530(b).

79. Inmediata 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).

80. As described before, Inmediata is also required (by the CCRA, CMIA and various other states' laws and regulations) to protect Plaintiffs' and Class Members' Personal and Medical Information, and further, to handle any breach of the same in accordance with applicable breach notification statutes.

81. In addition to its obligations under federal and state laws, Inmediata owed a duty to Plaintiffs and Class Members whose Personal and Medical Information was entrusted to Inmediata 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, disclosed, accessed, viewed, and/or

misused by unauthorized persons. Inmediata owed a duty to Plaintiffs and Class Members to provide reasonable security, including consistency with industry standards and requirements, and to ensure that its computer systems and networks, and the personnel responsible for them, adequately protected the Personal and Medical Information of Plaintiffs and Class Members.

82. Inmediata owed a duty to Plaintiffs and Class Members whose Personal and Medical Information was entrusted to Inmediata to design, maintain, and test its computer systems to ensure that the Personal and Medical Information in Inmediata's possession was adequately secured and protected.

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

84. Inmediata owed a duty to Plaintiffs and Class Members whose Personal and Medical Information was entrusted to Inmediata to implement processes that would detect a breach or leak on its data security systems in a timely manner.

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

86. Inmediata owed a duty to Plaintiffs and Class Members whose Personal and Medical Information was entrusted to Inmediata to adequately train and supervise its employees to detect a breach or leak on its data security systems in a timely manner.

87. Inmediata owed a duty to Plaintiffs and Class Members whose Personal and Medical Information was entrusted to Inmediata to disclose if its computer systems and data security practices were inadequate to safeguard Plaintiffs' and Class Members' Personal and Medical Information from exfiltration or leaks because such an inadequacy

would be a material fact in the decision to entrust Personal and Medical Information with Inmediata.

88. Inmediata owed a duty to Plaintiffs and Class Members whose Personal and Medical Information was entrusted to Inmediata to disclose in a timely and accurate manner when data breaches or leaks occurred.

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

Inmediata Was on Notice of Data Breach Threats and the Inadequacy of Its Data Security

90. Inmediata was on notice that companies in the healthcare industry were targets for cyberattacks.

91. Inmediata was on notice that the FBI has 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)."[4]

92. The American Medical Association ("AMA") has also warned healthcare companies about the importance of protecting their 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 practice that has experienced some kind of cyberattack. Unfortunately, practices are learning that cyberattacks not only

[4] Jim Finkle, *FBI Warns Healthcare Firms that they are Targeted by Hackers*, Reuters (Aug. 2014), https://www.reuters.com/article/us-cybersecurity-healthcare-fbi/fbi-warns-healthcare-firms-they-are-targeted-by-hackers-idUSKBN0GK24U20140820 (last visited May 18, 2020).

> threaten the privacy and security of patients' health and financial information, but also patient access to care.[5]

93. As implied by the above quote from the AMA, stolen Personal and Medical Information can be used to interrupt important medical services themselves. This is an imminent and certainly impending risk for all Plaintiffs and Class Members.

94. Inmediata was on notice that the federal government has been concerned about healthcare company data encryption. Inmediata knew it kept protected health information in its computer systems and yet did not encrypt its computer systems.

95. 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."[6]

96. As a covered entity or business associate under HIPAA, Inmediata should have known about its weakness toward data security threats and sought better protection for the Personal and Medical Information in its computer systems.

---

[5] 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-ransomware-attacks-shut-down-clinics-hospitals (last visited May 18, 2020).

[6] *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/3926/20150618190135/http://www.hhs.gov/news/press/2014pres/04/20140422b.html (last visited May 18, 2020).

It is Well Established That Data Breaches Lead to Identity Theft and Other Harms

97. Plaintiffs and Class Members have been injured by the release, disclosure and exfiltration of their Personal and Medical Information in the Data Breach.

98. Each year, identity theft causes tens of billions of dollars of losses to victims in the United States.[7] Cyber criminals can leverage Plaintiffs' and Class Members' Personal and Medical Information that was released, disclosed, and exfiltrated in the Data Breach to commit thousands of crimes, including opening new financial accounts in Plaintiffs' and Class Members' names, taking out loans in Plaintiffs' and Class Members' names, using Plaintiffs' and Class Members' names to obtain medical services, using Plaintiffs' and Class Members' Personal Information to file fraudulent tax returns, using Plaintiffs' and Class Members' health insurance information to rack up medical debts in their names, using Plaintiffs' and Class Members' health information to target them in other phishing and hacking intrusions based on their individual health needs, using Plaintiffs' and Class Members' information to obtain government benefits, obtaining driver's licenses in Plaintiffs' and Class Members' names but with another person's photograph, and giving false information to police during an arrest. Even worse, Plaintiffs and Class Members could be arrested for crimes identity thieves have committed.

99. 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.

[7] *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") (last visited May 18, 2020).

100. This is not just speculative. As the FTC has reported, if hackers get access to Personal and Medical Information, they ***will*** use it.[8]

101. For instance, with a stolen social security number, which is part of the Personal and Medical Information compromised in the Data Breach for some Class Members, someone can open financial accounts, get medical care, file fraudulent tax returns, commit crimes, and steal benefits.[9] Identity thieves can also use the information to qualify for expensive medical care and leave them and their contracted health insurers on the hook for massive medical bills.

102. 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."[10]

103. "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."[11]

---

[8] 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 (last visited May 18, 2020).

[9] *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/ (last visited May 18, 2020).

[10] Michael Ollove, "The Rise of Medical Identity Theft in Healthcare," Kaiser Health News, Feb. 7, 2014, https://khn.org/news/rise-of-indentity-theft/ (last visited May 18, 2020).

[11] *Id.*

104. 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 [(referring to prices on dark web marketplaces)]."[12] A complete identity theft kit that includes health insurance credentials may be worth up to $1,000 on the black market.[13]

105. If, moreover, cyber criminals also manage to acquire financial information, credit and debit cards, health insurance information, driver's licenses and passports, there is no limit to the amount of fraud to which Inmediata has exposed the Plaintiffs and Class Members.

106. The United States Government Accountability Office noted in a June 2007 report on Data Breaches ("GAO Report") that identity thieves use identifying data such as Social Security Numbers to open financial accounts, receive government benefits and incur charges and credit in a person's name.[14] As the GAO Report states, this type of identity theft is the most harmful because it often takes some time for the victim to become aware of the theft, and the theft can impact the victim's credit rating adversely.

---

[12]IDExperts, *You Got It, They Want It: Criminals Targeting Your Private Healthcare Data, New Ponemon Study Shows*, https://www.idexpertscorp.com/knowledge-center/single/you-got-it-they-want-it-criminals-are-targeting-your-private-healthcare-dat (last visited May 18, 2020).

[13]*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 (last visited May 18, 2020).

[14] *See Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown* (June 2007), United States Government Accountability Office, *available at* https://www.gao.gov/new.items/d07737.pdf (last visited May 18, 2020).

107. In addition, the GAO Report states that victims of identity theft will face "substantial costs and inconveniences repairing damage to their credit records" and their "good name."[15]

108. Identity theft victims are frequently required to spend many hours and large amounts of money repairing the impact to their credit. Identity thieves use stolen personal information for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud.

109. There may be a time lag between when sensitive personal information is stolen and when it is used. According to the GAO Report:

> [L]aw enforcement officials told us that in some cases, ***stolen data may be held for up to a year or more before being used to commit identity theft***. Further, once stolen data have been sold or posted on the Web, ***fraudulent use of that information may continue for years***. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[16]

110. With access to an individual's Personal and Medical Information, criminals can do more than just empty a victim's bank account – they can also commit all manner of fraud, including: obtaining a driver's license or official identification card in the victim's name but with the thief's picture; using the victim's name and Social Security Number to obtain government benefits; or, filing a fraudulent tax return using the victim's information. In addition, identity thieves may obtain a job using the victim's Social Security Number, rent a house, or receive medical services in the victim's name, and may

---

[15] *Id.* at 2, 9.
[16] *Id*. at 29 (emphasis added).

even give the victim's personal information to police during an arrest, resulting in an arrest warrant being issued in the victim's name.[17]

111. 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. As a result of recent large-scale data breaches, identity thieves and cyber criminals have openly posted stolen credit card numbers, Social Security Numbers, and other Personal and Medical Information directly on various Internet websites making the information publicly available.

112. A study by Experian found that the "average total cost" of medical identity theft is "about $20,000" per incident, and that a majority of victims of medical identity theft were forced to pay out-of-pocket costs for healthcare they did not receive in order to restore coverage.[18] Indeed, data breaches and identity theft have a crippling effect on individuals and detrimentally impact the entire economy as a whole.

113. Medical computer systems are especially valuable to identity thieves. According to a 2012 Nationwide Insurance report, "[a] stolen medical identity has a $50 street value – whereas a stolen social security number, on the other hand, only sells for $1."[19] In fact, the medical industry has experienced disproportionally higher instances of computer theft than any other industry.

---

[17] *See* Federal Trade Commission, *Warning Signs of Identity Theft*, *available at* https://www.identitytheft.gov/Warning-Signs-of-Identity-Theft (last visited May 18, 2020).

[18] *See* Elinor Mills, Study: Medical identity theft is costly for victims, CNET (Mar. 3, 2010), https://www.cnet.com/news/study-medical-identity-theft-is-costly-for-victims/ (last visited May 18, 2020).

[19] Study: Few Aware of Medical Identity Theft Risk, Claims Journal, https://www.claimsjournal.com/news/national/2012/06/14/208510.htm (last visited May 18, 2020).

114. Furthermore, identity theft victims must spend countless hours and large amounts of money repairing the impact to their credit.[20]

115. To date, Inmediata does not appear to be taking any measures to assist many affected Plaintiffs and similarly situated Class Members other than telling them to simply do the following:

- "remain vigilant";
- "review[] your account statements regularly and credit reports closely";
- "keep[] a close eye on your credit card activity";
- "promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities";
- obtain a copy of free credit reports;
- contact the FTC and/or the state Attorney General's office;
- enact a security freeze on credit files; and
- create a fraud alert.

None of these recommendations, however, require Inmediata to expend any effort, or take reasonable measures, to protect Plaintiffs' and Class Members' Personal and Medical Information.

116. Inmediata's failure to adequately protect Plaintiffs' and Class Members' Personal and Medical Information has resulted in Plaintiffs and Class Members having to undertake these tasks, which require extensive amounts of time, calls, and, for many of the credit and fraud protection services, payment of money—while Inmediata sits by and does nothing to assist those affected by the incident. Instead, as Inmediata's letter

[20] "Guide for Assisting Identity Theft Victims," Federal Trade Commission, 4 (Sept. 2013), https://www.consumer.ftc.gov/articles/pdf-0119-guide-assisting-id-theft-victims.pdf (last visited May 18, 2020).

indicates, it is putting the burden on the Plaintiffs and Class Members to discover possible fraudulent activity and identity theft.

117. Inmediata's offer of 12 months of identity monitoring *only* to Plaintiffs and Class Members whose Social Security Numbers it admits were involved in the Data Breach – and ***nothing*** to Plaintiffs and other Class Members whose Social Security Numbers it does not admit were involved—is woefully inadequate. While some harm has already begun to occur, the worst may be yet to come. There may be a time lag between when harm occurs versus when it is discovered, and also between when Personal and Medical Information is acquired and when it is used. Furthermore, identity monitoring only alerts someone to the fact that they have already been the victim of identity theft (*i.e.*, fraudulent acquisition and use of another person's Personal and Medical Information)—it does not prevent identity theft.[21] This is especially true for many kinds of medical identity theft, for which most credit monitoring plans provide little or no monitoring or protection.

118. As a direct and proximate result of the Data Breach, Plaintiffs and Class Members have been placed at an imminent, immediate, and continuing increased risk of harm from fraud and identity theft. Plaintiffs and Class Members must now take the time and effort to mitigate the actual and potential impact of the Data Breach 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.

---

[21] *See, e.g.*, Kayleigh Kulp, *Credit Monitoring Services May Not Be Worth the Cost*, Nov. 30, 2017, https://www.cnbc.com/2017/11/29/credit-monitoring-services-may-not-be-worth-the-cost.html (last visited May 18, 2020).

119. Plaintiffs and the Class Members have suffered, continue to suffer and/or will 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 release and 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;

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

e. Damages flowing from Inmediata's untimely and inadequate notification of the Data Breach;

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

g. Out-of-pocket expenses and the value of their time reasonably expended to remedy or mitigate the effects of the Data Breach;

h. Deprivation of the value of Plaintiffs' and Class Members' Personal and Medical 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.

120. Moreover, Plaintiffs and Class Members have an interest in ensuring that their information, which remains in the possession of Inmediata, is protected from further breaches by the implementation of security measures and safeguards.

Plaintiffs' Experiences

Plaintiff Vicki Stasi

121. Inmediata received and collected Ms. Stasi's Personal and Medical Information, which Inmediata maintained in its computer systems. Inmediata disclosed Ms. Stasi's name, address, date of birth, gender, and medical claim information including dates of service, diagnosis codes, procedure codes and treating physician to unauthorized third parties as a result of the Data Breach.

122. At the end of April 2019, Ms. Stasi received a letter dated April 22, 2019, from Inmediata notifying her of the of the Data Breach. *See* **Exhibit 3** (Letter from Inmediata CEO Mark Rieger to Vicki Stasi, dated April 22, 2019).

123. The Letter from Inmediata CEO Mark Rieger to Vicki Stasi stated that Ms. Stasi's "name, address, date of birth, gender, and medical claim information including dates of service, diagnosis codes, procedure codes and treating physician" were all compromised in the Data Breach. *Id.*

124. The Letter from Inmediata CEO Mark Rieger to Vicki Stasi was sent in accordance with 45 CFR § 164.404.

125. Pursuant to 45 CFR § 164.404, data breach notification letters are sent "following the discovery of a breach of unsecured protected health information" to "each individual whose unsecured protected health information has been, or is reasonably believed by the covered entity to have been, accessed, acquired, used, or disclosed as a result of such breach."

126. 45 CFR § 164.402 defines "breach" as "the acquisition, access, use, or disclosure of protected health information in a manner not permitted under subpart E of this part which compromises the security or privacy of the protected health information."

127. 45 CFR § 164.402 defines "unsecured protected health information" as "protected health information that is not rendered unusable, unreadable, or indecipherable to unauthorized persons through the use of a technology or methodology specified by the [HHS] Secretary."

128. Accordingly, Ms. Stasi's unsecured protected health information has been accessed, acquired, used, or disclosed in a manner not permitted under 45 CFR Subpart E as a result of the Data Breach.

129. Inmediata reasonably believes Ms. Stasi's unsecured protected health information has been, accessed, acquired, used, or disclosed in a manner not permitted under 45 CFR Subpart E as a result of the Data Breach.

130. Ms. Stasi's unsecured protected health information was acquired, accessed, used, or disclosed in a manner not permitted under 45 CFR Subpart E as a result of the Data Breach was not rendered unusable, unreadable, or indecipherable to unauthorized persons.

131. Inmediata reasonably believes Ms. Stasi's unsecured protected health information was acquired, accessed, used, or disclosed in a manner not permitted under 45 CFR Subpart E as a result of the Data Breach was not rendered unusable, unreadable, or indecipherable to unauthorized persons.

132. Ms. Stasi's unsecured protected health information was viewed by unauthorized persons in a manner not permitted under 45 CFR Subpart E as a result of the Data Breach.

133. Inmediata reasonably believes Ms. Stasi's unsecured protected health information was viewed by unauthorized persons in a manner not permitted under 45 CFR Subpart E as a result of the Data Breach.

134. It is reasonable to infer that Ms. Stasi's unsecured protected health information that was acquired, accessed, used, or disclosed in a manner not permitted under 45 CFR Subpart E as a result of the Data Breach, and which was not rendered unusable, unreadable, or indecipherable to unauthorized persons, was viewed by unauthorized persons.

135. It should be rebuttably presumed that Ms. Stasi's unsecured protected health information acquired, accessed, used, or disclosed in a manner not permitted under 45

CFR Subpart E, and which was not rendered unusable, unreadable, or indecipherable to unauthorized persons, was viewed by unauthorized persons.

136. Since approximately early 2019, Ms. Stasi has noticed an increase in spam/phishing emails from persons apparently attempting to defraud her.

137. Ms. Stasi now engages in monthly monitoring of her credit reports and weekly monitoring of her credit cards and bank accounts.

138. Ms. Stasi also received an improperly addressed letter for another individual affected by the Data Breach—the improperly addressed letter included Ms. Stasi's address, but the name of an individual not residing at Ms. Stasi's address.

139. Ms. Stasi has spent approximately 20 hours of her own time attempting to determine how she is connected to Inmediata, how her information came into the possession of Inmediata, and trying to make sure she has not and does not become further victimized because of the Data Breach.

140. As the recipient of a letter sent pursuant to California Civ. Code § 1798.82(a)(1)—and filed with the Attorney General of California in accordance with California Civ. Code § 1798.82(f)—it is and was reasonable for Ms. Stasi to believe that future harm (including identity theft) is and was real and imminent, and to take steps to mitigate that risk of future harm.

141. After receiving notice that she was the victim of a data breach that required the filing of a Breach Report in accordance with 45 CFR § 164.408(a), it is and was reasonable for Ms. Stasi to believe that future harm (including identity theft) is and was real and imminent, and to take steps to mitigate that risk of future harm.

Plaintiff Shane White

142. Inmediata received and collected Mr. White's Personal and Medical Information, which Inmediata maintained in its computer systems. Inmediata disclosed Mr. White's name, address, date of birth, gender, and medical claim information including dates of service, diagnosis codes, procedure codes and treating physician to unauthorized third parties as a result of the Data Breach.

143. In approximately late April of 2019, Mr. White received a letter dated April 22, 2019, from Inmediata notifying him of the of the Data Breach. *See* **Exhibit 4** (Letter from Inmediata CEO Mark Rieger to Shane White, dated April 22, 2019).

144. The Letter from Inmediata CEO Mark Rieger to Shane White stated that Mr. White's "name, address, date of birth, gender, and medical claim information including dates of service, diagnosis codes, procedure codes and treating physician" were all compromised in the Data Breach. *Id.*

145. The Letter from Inmediata CEO Mark Rieger to Shane White was sent in accordance with 45 CFR § 164.404.

146. Pursuant to 45 CFR § 164.404, data breach notification letters are sent "following the discovery of a breach of unsecured protected health information" to "each individual whose unsecured protected health information has been, or is reasonably believed by the covered entity to have been, accessed, acquired, used, or disclosed as a result of such breach."

147. 45 CFR § 164.402 defines "breach" as "the acquisition, access, use, or disclosure of protected health information in a manner not permitted under subpart E of this part which compromises the security or privacy of the protected health information."

148. 45 CFR § 164.402 defines "unsecured protected health information" as "protected health information that is not rendered unusable, unreadable, or indecipherable to unauthorized persons through the use of a technology or methodology specified by the [HHS] Secretary."

149. Accordingly, Mr. White's unsecured protected health information has been accessed, acquired, used, or disclosed in a manner not permitted under 45 CFR Subpart E as a result of the Data Breach.

150. Inmediata reasonably believes Mr. White's unsecured protected health information has been, accessed, acquired, used, or disclosed in a manner not permitted under 45 CFR Subpart E as a result of the Data Breach.

151. Mr. White's unsecured protected health information acquired, accessed, used, or disclosed in a manner not permitted under 45 CFR Subpart E as a result of the Data Breach was not rendered unusable, unreadable, or indecipherable to unauthorized persons.

152. Inmediata reasonably believes Mr. White's unsecured protected health information acquired, accessed, used, or disclosed in a manner not permitted under 45 CFR Subpart E as a result of the Data Breach was not rendered unusable, unreadable, or indecipherable to unauthorized persons.

153. Mr. White's unsecured protected health information was viewed by unauthorized persons in a manner not permitted under 45 CFR Subpart E as a result of the Data Breach.

154. Inmediata reasonably believes Mr. White's unsecured protected health information was viewed by unauthorized persons in a manner not permitted under 45 CFR Subpart E as a result of the Data Breach.

155. It is reasonable to infer that Mr. White's unsecured protected health information that was acquired, accessed, used, or disclosed in a manner not permitted under 45 CFR Subpart E as a result of the Data Breach, and which was not rendered unusable, unreadable, or indecipherable to unauthorized persons, was viewed by unauthorized persons.

156. It should be rebuttably presumed that Mr. White's unsecured protected health information acquired, accessed, used, or disclosed in a manner not permitted under 45 CFR Subpart E, and which was not rendered unusable, unreadable, or indecipherable to unauthorized persons, was viewed by unauthorized persons.

157. Since approximately early 2019, Mr. White has noticed a sharp increase in spam/phishing calls from persons apparently attempting to defraud him.

158. Mr. White has spent approximately 2 hours of his own time attempting to determine how he is connected to Inmediata and how his information came into the possession of Inmediata.

159. On or about September 27, 2019, Mr. White learned that he had been the victim of multiple fraudulent charges in an amount totaling more than $600 on his credit card. As a result of the fraudulent charges, Mr. White's credit card was cancelled, and he was without access to the use of his credit card until it was replaced.

160. The credit card that incurred the fraudulent charges was used as a method of payment at not less than five different healthcare and dentalcare providers along with two health and dental insurance companies.

161. This credit card had not previously experienced any fraudulent charges and, other than the Equifax data breach of 2017, Mr. White has not received any other data breach notices.

162. Given the fact that Mr. White received a Data Breach notice from Inmediata and that one of Inmediata's primary roles is as a billing processor and facilitator for hospitals, physicians, dentists, and other healthcare related professionals and entities, Mr. White believes Inmediata was the source of his breached credit card information.

163. Mr. White was exposed to and experienced actual fraud, and as a result of having been victimized by the Data Breach, Mr. White was required to spend approximately 3 to 4 hours dealing with the aftermath of the Data Breach.

164. As the recipient of a letter sent pursuant to California Civ. Code § 1798.82(a)(1)—and filed with the Attorney General of California in accordance with California Civ. Code § 1798.82(f) —it is and was reasonable for Mr. White to believe that future harm (including identity theft) is and was real and imminent, and to take steps to mitigate that risk of future harm.

165. After receiving notice that he was the victim of a data breach that required the filing of a Breach Report in accordance with 45 CFR § 164.408(a), it is and was reasonable for Mr. White to believe that future harm (including identity theft) is and was real and imminent, and to take steps to mitigate that risk of future harm.

Plaintiff Crystal Garcia

166. Inmediata received and collected Ms. Garcia's Personal and Medical Information, which Inmediata maintained in its computer systems. Inmediata disclosed Ms. Garcia's name, address, date of birth, gender, and medical claim information including dates of service, diagnosis codes, procedure codes and treating physician to unauthorized third parties as a result of the Data Breach.

167. In April of 2019, Ms. Garcia received a letter dated April 22, 2019, from Inmediata notifying her of the of the Data Breach. *See* **Exhibit 5** (Letter from Inmediata CEO Mark Rieger to Crystal Garcia, dated April 22, 2019).

168. The Letter from Inmediata CEO Mark Rieger to Crystal Garcia stated that Ms. Garcia's "name, address, date of birth, gender, and medical claim information including dates of service, diagnosis codes, procedure codes and treating physician" were all compromised in the Data Breach. *Id.*

169. The Letter from Inmediata CEO Mark Rieger to Crystal Garcia was sent in accordance with 45 CFR § 164.404.

170. Pursuant to 45 CFR § 164.404, data breach notification letters are sent "following the discovery of a breach of unsecured protected health information" to "each individual whose unsecured protected health information has been, or is reasonably believed by the covered entity to have been, accessed, acquired, used, or disclosed as a result of such breach."

171. 45 CFR § 164.402 defines "breach" as "the acquisition, access, use, or disclosure of protected health information in a manner not permitted under subpart E of this part which compromises the security or privacy of the protected health information."

172. 45 CFR § 164.402 defines "unsecured protected health information" as "protected health information that is not rendered unusable, unreadable, or indecipherable to unauthorized persons through the use of a technology or methodology specified by the [HHS] Secretary."

173. Accordingly, Ms. Garcia's unsecured protected health information has been accessed, acquired, used, or disclosed in a manner not permitted under 45 CFR Subpart E as a result of the Data Breach.

174. Inmediata reasonably believes Ms. Garcia's unsecured protected health information has been, accessed, acquired, used, or disclosed in a manner not permitted under 45 CFR Subpart E as a result of the Data Breach.

175. Ms. Garcia's unsecured protected health information acquired, accessed, used, or disclosed in a manner not permitted under 45 CFR Subpart E as a result of the Data Breach was not rendered unusable, unreadable, or indecipherable to unauthorized persons.

176. Inmediata reasonably believes Ms. Garcia's unsecured protected health information acquired, accessed, used, or disclosed in a manner not permitted under 45 CFR Subpart E as a result of the Data Breach was not rendered unusable, unreadable, or indecipherable to unauthorized persons.

177. Ms. Garcia's unsecured protected health information was viewed by unauthorized persons in a manner not permitted under 45 CFR Subpart E as a result of the Data Breach.

178. Inmediata reasonably believes Ms. Garcia's unsecured protected health information was viewed by unauthorized persons in a manner not permitted under 45 CFR Subpart E as a result of the Data Breach.

179. It is reasonable to infer that Ms. Garcia's unsecured protected health information that was acquired, accessed, used, or disclosed in a manner not permitted under 45 CFR Subpart E as a result of the Data Breach, and which was not rendered unusable, unreadable, or indecipherable to unauthorized persons, was viewed by unauthorized persons.

180. It should be rebuttably presumed that Ms. Garcia's unsecured protected health information acquired, accessed, used, or disclosed in a manner not permitted under

45 CFR Subpart E, and which was not rendered unusable, unreadable, or indecipherable to unauthorized persons, was viewed by unauthorized persons.

181. The Letter from Inmediata CEO Mark Rieger to Crystal Garcia was sent in accordance with California Civ. Code § 1798.82(a)(1).

182. 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".

183. 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."

184. Thus, Ms. Garcia's unencrypted personal information was acquired by an unauthorized person as a result of the Data Breach.

185. Inmediata reasonably believes Ms. Garcia's unencrypted personal information was acquired by an unauthorized person as a result of the Data Breach.

186. The security, confidentiality, or integrity of Ms. Garcia's unencrypted personal information was compromised by Inmediata as a result of the Data Breach.

187. Inmediata reasonably believes the security, confidentiality, or integrity of Ms. Garcia's unencrypted personal information was compromised by Inmediata as a result of the Data Breach.

188. Ms. Garcia's unencrypted personal information that was acquired by an unauthorized person as a result of the Data Breach, was viewed by unauthorized persons.

189. Inmediata reasonably believes Ms. Garcia's unencrypted personal information that was acquired by an unauthorized person as a result of the Data Breach, was viewed by unauthorized persons.

190. It is reasonable to infer that Ms. Garcia's unencrypted personal information that was acquired by an unauthorized person as a result of the Data Breach, was viewed by unauthorized persons.

191. It should be rebuttably presumed that Ms. Garcia's unencrypted personal information that was acquired by an unauthorized person as a result of the Data Breach, was viewed by unauthorized persons.

192. Over approximately the past year, Ms. Garcia has noticed an increase in spam/phishing calls and emails from persons apparently attempting to defraud her.

193. After being notified of the breach, Ms. Garcia placed credit freezes on her credit reports with the three major U.S. consumer credit reporting agencies in order to detect potential identity theft and fraudulent activity.

194. Ms. Garcia now engages in monthly monitoring of her credit and her bank accounts.

195. As a result of the Data Breach, Ms. Garcia has spent her own money and numerous hours addressing issues arising from the Data Breach.

196. As the recipient of a letter sent pursuant to California Civ. Code § 1798.82(a)(1) – and filed with the Attorney General of California in accordance with California Civ. Code § 1798.82(f) – it is and was reasonable for Ms. Garcia to believe that future harm (including identity theft) is and was real and imminent, and to take steps to mitigate that risk of future harm.

197. After receiving notice that she was the victim of a data breach that required the filing of a Breach Report in accordance with 45 CFR § 164.408(a), it is and was reasonable for Ms. Garcia to believe that future harm (including identity theft) is and was real and imminent, and to take steps to mitigate that risk of future harm.

CLASS ALLEGATIONS

198. Plaintiffs bring this class action lawsuit on behalf of themselves and the proposed Class Members under Rule 23 of the Federal Rules of Civil Procedure.

199. Plaintiffs seek certification of a Nationwide Class, a California Sub-Class, a Florida Sub-Class, and a Minnesota Sub-Class defined as follows:

> Nationwide Class: All persons in the United States whose Personal and Medical Information was compromised as a result of the Data Breach announced by Inmediata on or around April 24, 2019.

200. In the alternative to the Nationwide Class, Plaintiffs seek certification of the following state classes:

> California Sub-Class: All persons in the State of California whose Personal and Medical Information was compromised as a result of the Data Breach announced by Inmediata on or around April 24, 2019.
>
> Florida Sub-Class: All persons in the State of Florida whose Personal and Medical Information was compromised as a result of the Data Breach announced by Inmediata on or around April 24, 2019.
>
> Minnesota Sub-Class: All persons in the State of Minnesota whose Personal and Medical Information was compromised as a result of the Data Breach announced by Inmediata on or around April 24, 2019.

201. Specifically excluded from the Classes are Defendant and any entities in which Defendant has a controlling interest, Defendant's agents and employees, the judge to whom this action is assigned, members of the judge's staff, and the judge's immediate family.

202. **Numerosity:** Plaintiffs do not know the exact number of Class Members, but believe the Classes comprise approximately 1.5 million individuals throughout the United States. As such, Class Members are so numerous that joinder of all members is impracticable.

203. **Commonality:** Common questions of law and fact exist and predominate over any questions affecting only individual Class Members. The common questions include:

a. Whether Defendant engaged in the conduct alleged herein;

b. Whether Defendant failed to adequately safeguard Plaintiffs' and Class Members' Personal and Medical Information;

c. Whether Defendant failed to protect Plaintiffs' and Class Members' Personal and Medical Information properly and/or as promised;

d. Whether Defendant's computer system and data security practices used to protect Plaintiffs' and the Class Members' Personal and Medical Information violated HIPAA, federal, state and local laws, or Defendant's duties;

e. Whether Defendant engaged in unfair, unlawful, or deceptive practices by failing to safeguard Plaintiffs' and Class Members' Personal and Medical Information;

f. Whether Defendant violated the consumer protection statutes, data breach notification statutes, state unfair insurance practice statutes, state insurance privacy statutes, and/or state medical privacy statutes applicable to Plaintiffs and Class Members;

g. Whether Defendant failed to notify Plaintiffs and Class Members about the Data Breach as soon as practical and without delay after the Data Breach was discovered;

h. Whether Defendant acted negligently in failing to safeguard Plaintiffs' and Class Members' Personal and Medical Information;

i. Whether Defendant express or implied contractual obligations to protect the confidentiality of Plaintiffs' and the Class Members' Personal and Medical Information, and to have reasonable data security measures;

j. Whether Defendant's conduct described herein constitutes a breach of contract with Plaintiffs and Class Members;

k. Whether Plaintiffs and Class Members are entitled to damages as a result of Defendant's wrongful conduct;

l. Whether Plaintiffs and Class Members are entitled to restitution as a result of Defendant's wrongful conduct;

m. What equitable relief is appropriate to redress Defendant's wrongful conduct; and

n. What injunctive relief is appropriate to redress the imminent and currently ongoing harm faced by Plaintiffs and Class Members.

204. **Typicality:** Plaintiffs' claims are typical of the claims of the Class Members. Plaintiffs and Class Members were injured through Defendant's uniform misconduct and their legal claims arise from the same core practices of Defendant.

205. **Adequacy:** Plaintiffs will fairly and adequately represent and protect the interests of the Classes, and have retained counsel competent and experienced in complex litigation and class actions. Plaintiffs have no interests antagonistic to those of the Classes, and there are no defenses unique to Plaintiffs. Plaintiffs and their counsel are committed to prosecuting this action vigorously on behalf of the members of the proposed Classes, and have the financial resources to do so. Neither Plaintiffs nor their counsel have any interest adverse to those of the other members of the Classes.

206. **Risks:** The proposed action meets the requirements of Fed. R. Civ. P. 23 because prosecution of separate actions by individual members of the Classes would create a risk of inconsistent or varying adjudications that would establish incompatible standards for Defendant or would be dispositive of the interests of members of the proposed Classes. Furthermore, the Inmediata Database still exists, and is still vulnerable to future attacks – one standard of conduct is needed to ensure the future safety of the Inmediata Database.

207. **Injunctive Relief:** The proposed action meets the requirements of Fed. R. Civ. P. 23(b)(2) because Defendant has acted or has refused to act on grounds generally

applicable to the Classes, so that final injunctive relief or corresponding declaratory relief is appropriate as to the Classes as a whole.

208. **Predominance:** The proposed action meets the requirements of Fed. R. Civ. P. 23(b)(3) because questions of law and fact common to the Classes predominate over any questions that may affect only individual Class Members in the proposed Classes.

209. **Superiority:** The proposed action also meets the requirements of Fed. R. Civ. P. 23(b)(3) because a class action is superior to all other available methods of fairly and efficiently adjudicating this dispute. The injury sustained by each Class Member, while meaningful on an individual basis, is not of such magnitude that it is economically feasible to prosecute individual actions against Defendant. Even if it were economically feasible, requiring more than 1.5 million injured plaintiffs to file individual suits would impose a crushing burden on the court system and almost certainly lead to inconsistent judgments. By contrast, class treatment will present far fewer management difficulties and provide the benefits of a single adjudication, economies of scale, and comprehensive supervision by a single court. Plaintiffs anticipate no unusual difficulties in managing this class action.

210. **Certification of Particular Issues:** In the alternative, this action may be maintained as class action with respect to particular issues, in accordance with Fed. R. Civ. P. 23(c)(4).

211. Finally, all members of the purposed Classes are readily ascertainable. Defendant has access to addresses and other contact information for members of the Classes, which can be used to identify Class Members.

COUNT I

NEGLIGENCE

212. Plaintiffs reallege and incorporate by reference every allegation set forth in the preceding paragraphs as though alleged in this Count.

213. This count is brought on behalf of all Classes.

214. Inmediata solicited, collected, and stored the Personal and Medical Information of Plaintiffs and Class Members.

215. Inmediata knew, or should have known, of the risks inherent in collecting and storing Plaintiffs' and Class Members' Personal and Medical Information and the importance of adequate security.

216. Inmediata was well aware of the fact that hackers routinely attempt to access Personal and Medical Information without authorization. Inmediata also knew about numerous, well-publicized data breaches wherein hackers stole the Personal and Medical Information from companies who held or stored such information.

217. Inmediata owed duties of care to Plaintiffs and Class Members whose Personal and Medical Information had been entrusted with Inmediata.

218. Inmediata owed a common law duty to use reasonable care to avoid causing foreseeable risk of harm to Plaintiffs and Class Members when obtaining, storing, using, and managing Personal and Medical Information, including taking action to reasonably safeguard such data and providing notification to Plaintiff and Class Members of any breach in a timely manner so that appropriate action could be taken to minimize or avoid losses.

219. This duty extends to protecting others 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.

220. Plaintiffs and Class Members were the intended beneficiaries of Inmediata's duty to safeguard their Personal and Medical Information, creating a "special relationship" between them and Inmediata. Only Inmediata was in a position to ensure that its systems were sufficient to protect Plaintiffs' and Class Members' Personal and Medical Information that was entrusted to it.

221. In addition to the general duties above, Defendant's duties specifically included the following:

a. To exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting and protecting Personal and Medical Information in its possession;

b. To protect Personal and Medical Information in its possession using reasonable and adequate security procedures and systems;

c. To adequately and properly audit, test, and train its employees regarding how to properly and securely transmit and store Personal and Medical Information;

d. To implement processes to quickly detect a data breach, security incident, or intrusion; and

e. To promptly notify Plaintiffs and Class Members of any data breach, security incident, or intrusion that affected or may have affected their Personal and Medical Information.

222. Inmediata had additional duties imposed by statute and regulation as discussed herein.

223. Pursuant to the Federal Trade Commission Act (15 U.S.C. § 45), Inmediata had a duty to provide fair and adequate computer systems and data security practices to safeguard Plaintiffs' and Class Members' Personal and Medical Information.

224. Pursuant to HIPAA (42 U.S.C. § 1302d et. seq.), Inmediata had a duty to implement reasonable safeguards to protect Plaintiffs' and Class Members' Personal and Medical Information.

225. Pursuant to the Gramm-Leach-Bliley Act (15 U.S.C. § 6801), Inmediata had a duty to protect the security and confidentiality of Plaintiffs' and Class Members' Personal and Medical Information.

226. Pursuant to Fla. Stat. § 501.171(2), Cal. Civ. Code § 56 *et seq.*, and Minn. Stat. §144.291 *et seq.*, Inmediata had a duty to implement and maintain reasonable

security procedures and practices to safeguard Plaintiffs' and Class Members' Personal and Medical Information.

227. Inmediata breached its duties to Plaintiffs and Class Members under the Federal Trade Commission Act (15 U.S.C. § 45), HIPAA (42 U.S.C. § 1302d et. seq.), Gramm- Leach-Bliley Act (15 U.S.C. § 6801), Fla. Stat. § 501.171(2), Cal. Civ. Code § 56 *et seq.*, and Minn. Stat. §144.291 *et seq.* by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiffs' and Class Members' Personal and Medical Information.

228. Plaintiffs and Class Members are within the class of persons these statutes and their regulations were intended to protect. The harms which occurred, including the loss of privacy, significant risk of identity theft, and overpayment for goods and services, are the types of harm that these statutes and their regulations were intended to prevent.

229. Inmediata violated these statutes when it engaged in the actions and omissions alleged herein. Plaintiffs' and Class Members' injuries were a direct and proximate result of Inmediata's violations of these statutes. Plaintiffs and Class Members are therefore are entitled to the evidentiary presumptions in Cal. Evid. Code § 669 and for negligence *per se*.

230. It was foreseeable that injury to Plaintiffs and Class Members would result from Inmediata's violation of these duties in mishandling Plaintiffs' and Class Members' Personal and Medical Information.

231. Because Inmediata knew that a security incident, breach or intrusion upon its systems would potentially damage hundreds of thousands of individuals, including Plaintiffs and Class Members, it had a duty to adequately protect their Personal and Medical Information.

232. Inmediata knew, or should have known, that its security practices and computer systems did not adequately safeguard Plaintiffs' and Class Members' Personal and Medical Information.

233. Inmediata breached its duties of care by failing to provide fair, reasonable, or adequate computer systems and security practices to safeguard Plaintiffs' and Class Members' Personal and Medical Information.

234. Inmediata breached its duties of care by failing to provide prompt notice of the Data Breach to Plaintiffs and Class Members.

235. Inmediata acted with reckless disregard for the security of Plaintiffs' and Class Members' Personal and Medical Information because Defendant knew or should have known that its computer systems and data security practices were not adequate to safeguard the Personal and Medical Information that it collected and stored.

236. Inmediata acted with reckless disregard for the rights of Plaintiffs and Class Members by failing to provide prompt and adequate notice of the Data Breach so they could take measures to protect themselves from damages caused by the fraudulent use of Personal and Medical Information compromised in the Data Breach.

237. Inmediata had a "special relationship" with Plaintiffs and Class Members. The willingness to share and entrust Plaintiffs' and Class Members' Personal and Medical Information with Inmediata was predicated on the understanding that Inmediata would take adequate security precautions. Moreover, only Inmediata had the ability to protect its systems (and the Personal and Medical Information stored on them) and to implement security practices to protect the Personal and Medical Information it collected and stored.

238. Inmediata's own conduct also created a foreseeable risk of harm to Plaintiffs and Class Members and their Personal and Medical Information. Inmediata's misconduct included failing to:

a. Secure access to its servers;
b. Comply with current industry standard security practices;
c. Properly and adequately train employees on proper data security practices;
d. Implement adequate system and event monitoring;

e. Implement the systems, policies, and procedures necessary to prevent hackers from accessing and utilizing Personal and Medical Information transmitted and/or stored by Defendant;

f. Undertake periodic audits of record-keeping processes to evaluate the safeguarding of Personal and Medical Information;

g. Secure Personal and Medical Information and limit access to it to those with a legitimate business need;

h. Employ or contract with trained professionals to ensure security of network servers and evaluate the systems used to manage e-mail, Internet use, and so forth; and

i. Have a plan ready and in position to act quickly should a theft or data breach occur.

239. Inmediata also had independent duties under federal and state law requiring it to reasonably safeguard Plaintiffs' and Class Members' Personal and Medical Information and promptly notify them about the Data Breach.

240. Inmediata breached the duties it owed to Plaintiffs and Class Members in numerous ways, including:

a. By creating a foreseeable risk of harm through the misconduct previously described;

b. By failing to implement adequate security systems, protocols and practices sufficient to protect Plaintiffs' and Class Members' Personal and Medical Information both before and after learning of the Data Breach;

c. By failing to comply with the minimum industry data security standards before, during, and after the period of the Data Breach; and

d. By failing to timely and accurately disclose that Plaintiffs' and Class Members' Personal and Medical Information had been improperly

released, disclosed, used, acquired, accessed, and viewed in the Data Breach.

241. But for Inmediata's wrongful and grossly negligent breach of the duties it owed Plaintiffs and Class Members, their Personal and Medical Information either would not have been compromised or they would have been able to prevent some or all of their damages.

242. As a direct and proximate result of Inmediata's negligent conduct, Plaintiffs and Class Members have suffered damages and are at imminent risk of certainly impending future harm.

243. The injury and harm Plaintiffs and Class Members suffered (as alleged above) was and is reasonably foreseeable.

244. The injury and harm Plaintiffs and Class Members suffered (as alleged above) was the direct and proximate result of Inmediata's negligent conduct.

245. Plaintiffs and the Class Members have suffered injury and are entitled to damages in an amount to be proven at trial.

COUNT II

BREACH OF CONTRACTS TO WHICH PLAINTIFFS AND CLASS MEMBERS WERE INTENDED THIRD-PARTY BENEFICIARIES

246. Plaintiffs reallege and incorporate by reference every allegation set forth in the preceding paragraphs as though alleged in this Count.

247. This count is brought on behalf of all Classes.

248. Upon information and belief, Plaintiffs and Class Members are intended third-party beneficiaries of contracts entered into between Inmediata and its customers, including health plans, hospitals, IPAs, and independent physicians.

249. Upon further information and belief, these contracts and require, *inter alia*, that Inmediata take appropriate steps to safeguard the sensitive Personal and Medical Information entrusted to it by its customers that obtain that information from Plaintiffs and Class Members.

250. Plaintiffs and the Class Members are intended third party beneficiaries of these contracts. Under the circumstances, recognition of a right to performance by Plaintiffs and the Class Members is appropriate to effectuate the intentions of the parties to these contracts. One or more of the parties to these contracts intended to give Plaintiffs and the Class Members the benefit of the performance promised in the contracts.

251. Inmediata breached these agreements, which directly and/or proximately caused Plaintiffs and the Class Members to suffer substantial damages.

252. Upon further information and belief, Inmediata saved (or avoided spending) a substantial sum of money by knowingly failing to comply with its contractual obligations, and continues to do so.

253. Accordingly, Inmediata has been unjustly enriched and Plaintiffs and Class Members who have been injured are entitled to damages, restitution, disgorgement of profits and other relief in an amount to be proven at trial.

COUNT III

UNJUST ENRICHMENT

254. Plaintiffs reallege and incorporate by reference every allegation set forth in the preceding paragraphs as though alleged in this Count.

255. This count is brought in the alternative to Plaintiffs' breach of contract (third-party beneficiary) count.

256. This count is brought on behalf of all Classes.

257. Plaintiffs and Class Members conferred a monetary benefit on Inmediata. Inmediata received and retained money belonging to Plaintiffs and Class Members either directly through copayments and coinsurance or indirectly through health insurance/medical plans that they had paid for.

258. Inmediata had knowledge of the benefits conferred on it by Plaintiffs and the Class Members.

259. The money that Plaintiffs and Class members paid indirectly to Inmediata was supposed to be used by Inmediata, in part, to pay for the costs of HIPAA and CMIA compliance and reasonable data privacy and security practices and procedures.

260. As a result of Inmediata's conduct, Plaintiffs and Class members suffered damages in an amount equal to the difference in value between health care services with the reasonable data privacy and security practices and procedures that they paid for, and the inadequate health care services without reasonable data privacy and security practices and procedures that they received.

261. Under principals of equity and good conscience, Inmediata should not be permitted to retain the money belonging to Plaintiffs and Class members because Inmediata failed to implement (or to adequately implement) the data privacy and security practices and procedures that Plaintiffs and Class members paid for and that were otherwise mandated by HIPAA regulations, federal, state, and local laws, and industry standards.

262. Inmediata should be compelled to disgorge into a common fund for the benefit of Plaintiffs and Class members all unlawful or inequitable proceeds that Inmediata received.

263. A constructive trust should be imposed on all unlawful or inequitable sums received by Inmediata traceable to Plaintiffs and Class Members.

COUNT IV

VIOLATION OF CALIFORNIA'S

CONFIDENTIALITY OF MEDICAL INFORMATION ACT

Cal. Civ. Code § 56 *et seq.*

264. Plaintiffs reallege and incorporate by reference every allegation set forth in the preceding paragraphs as though alleged in this Count.

265. This count is brought on behalf of all Classes or, in the alternative, the California Sub-Class.

266. Inmediata is a "Contractor" as defined by Cal. Civ. Code § 56.05(d) and/or a "Provider of Health Care" as expressed in Cal. Civ. Code § 56.06, and is therefore subject to the requirements of the CMIA, Cal. Civ. Code §§ 56.10(a), (d) and (e), 56.101(a) and (b), 56.26(a), and 56.36(b).

267. Plaintiffs and Class Members are "Patients" as defined by Cal. Civ. Code § 56.05(k).

268. The Plaintiffs' and Class Members' Personal and Medical Information that was the subject of the Data Breach included "Medical Information" as defined by Cal. Civ. Code § 56.05(j).

269. In violation of Cal. Civ. Code § 56.10(a), Inmediata disclosed medical information (including Plaintiffs' and Class Members' Personal and Medical Information) without first obtaining an authorization. The unauthorized disclosure of Plaintiffs' and Class Members' Personal and Medical Information to unauthorized individuals in the Data Breach resulted from the affirmative actions of Inmediata's employees, who posted on the Internet Plaintiffs' and Class Members' Personal and Medical Information. Posting Plaintiffs' and Class Members' Personal and Medical Information on the Internet was an affirmative communicative act by Inmediata and a violation of Cal. Civ. Code § 56.10(a). Plaintiffs' and Class Members' Personal and Medical Information was viewed by unauthorized individuals as a direct and proximate result of Inmediata's violation of Cal. Civ. Code § 56.10(a).

270. In violation of the first sentence of Cal. Civ. Code § 56.101(a), Inmediata created, maintained, preserved, stored, abandoned, destroyed, or disposed of medical information (including Plaintiffs' and Class Members' Personal and Medical Information) in a manner that failed to preserve and breached the confidentiality of the information contained therein. This violation resulted from the affirmative actions of Inmediata's employees, who posted on the Internet Plaintiffs' and Class Members' Personal and Medical Information. Posting Plaintiffs' and Class Members' Personal and Medical Information on the Internet was an affirmative communicative act by Inmediata

and a violation of the first sentence of Cal. Civ. Code § 56.101(a). Plaintiffs' and Class Members' Personal and Medical Information was viewed by unauthorized individuals as a direct and proximate result of Inmediata's violation of the first sentence of Cal. Civ. Code § 56.101(a).

271. In violation of the second sentence of Cal. Civ. Code § 56.101(a), Inmediata negligently created, maintained, preserved, stored, abandoned, destroyed, or disposed of medical information (including Plaintiffs' and Class Members' Personal and Medical Information). This violation resulted from the affirmative actions of Inmediata's employees, who posted on the Internet Plaintiffs' and Class Members' Personal and Medical Information. Posting Plaintiffs' and Class Members' Personal and Medical Information on the Internet was an affirmative communicative act by Inmediata and a violation of the second sentence of Cal. Civ. Code § 56.101(a). Plaintiffs' and Class Members' Personal and Medical Information was viewed by unauthorized individuals as a direct and proximate result of Inmediata's violation of the second sentence of Cal. Civ. Code § 56.101(a).

272. The Plaintiffs' and Class Members' Personal and Medical Information that was the subject of the Data Breach included "electronic medical records" or "electronic health records" as referenced by Cal. Civ. Code § 56.101(c) and defined by 42 U.S.C. § 17921(5).

273. In violation of Cal. Civ. Code § 56.101(b)(1)(A), Inmediata's electronic health record system or electronic medical record system failed to protect and preserve the integrity of electronic medical information (including Plaintiffs' and Class Members' Personal and Medical Information). This violation resulted from the affirmative actions of Inmediata's employees, who posted on the Internet Plaintiffs' and Class Members' Personal and Medical Information. Posting Plaintiffs' and Class Members' Personal and Medical Information on the Internet was an affirmative communicative act by Inmediata and a violation of Cal. Civ. Code § 56.101(b)(1)(A). Plaintiffs' and Class Members'

Personal and Medical Information was viewed by unauthorized individuals as a direct and proximate result of Inmediata's violation of Cal. Civ. Code § 56.101(b)(1)(A).

274. In violation of Cal. Civ. Code § 56.101(b)(1)(B), Inmediata's electronic health record system or electronic medical record system failed to automatically record and preserve any change or deletion of any electronically stored medical information (including Plaintiffs' and Class Members' Personal and Medical Information).

275. In violation of Cal. Civ. Code § 56.101(b)(1)(B), Inmediata's electronic health record system or electronic medical record system failed to record the identity of persons who accessed and changed medical information (including Plaintiffs' and Class Members' Personal and Medical Information), failed to record the date and time medical information was accessed (including Plaintiffs' and Class Members' Personal and Medical Information), and failed to record changes that were made to medical information (including Plaintiffs' and Class Members' Personal and Medical Information).

276. In violation of Cal. Civ. Code § 56.26(a) Inmediata, as an entity engaged in the business of furnishing administrative services to programs that provide payment for health care services, knowingly used, disclosed, or permitted its employees or agents to use or disclose medical information (including Plaintiffs' and Class Members' Personal and Medical Information) possessed in connection with performing administrative functions for a program, in a manner not reasonably necessary in connection with the administration or maintenance of the program, or in a manner not required by law, or without authorization. This violation resulted from the affirmative actions of Inmediata's employees, who posted on the Internet Plaintiffs' and Class Members' Personal and Medical Information. Posting Plaintiffs' and Class Members' Personal and Medical Information on the Internet was an affirmative communicative act by Inmediata and a violation of Cal. Civ. Code § 56.26(a). Plaintiffs' and Class Members' Personal and Medical Information was viewed by unauthorized individuals as a direct and proximate result of Inmediata's violation of Cal. Civ. Code § 56.26(a).

277. In violation of Cal. Civ. Code § 56.36(b) Inmediata negligently released confidential information or records concerning Plaintiffs and Class Members (including Plaintiffs' and Class Members' Personal and Medical Information). This negligent release of Plaintiffs' and Class Members' Personal and Medical Information to unauthorized individuals in the Data Breach resulted from the affirmative actions of Inmediata's employees, who posted on the Internet Plaintiffs' and Class Members' Personal and Medical Information. Posting Plaintiffs' and Class Members' Personal and Medical Information on the Internet was an affirmative communicative act by Inmediata and a violation of Cal. Civ. Code § 56.36(b). Plaintiffs' and Class Members' Personal and Medical Information was viewed by unauthorized individuals as a direct and proximate result of Inmediata's violation of Cal. Civ. Code § 56.36(b).

278. In violation of Cal. Civ. Code § 56.10(d), Inmediata intentionally shared, sold, used for marketing, or otherwise used Plaintiffs' and Class Members' Personal and Medical Information for a purpose not necessary to provide health care services to Plaintiffs or Class Members.

279. In violation of Cal. Civ. Code § 56.10(e), Inmediata further disclosed Plaintiffs' and Class Members' Personal and Medical Information to persons or entities not engaged in providing direct health care services to Plaintiffs or Class Members or their providers of health care or health care service plans or insurers or self-insured employers.

280. All of Inmediata's acts described herein were done knowingly and willfully by Inmediata.

281. Plaintiffs and Class Members were injured and have suffered damages, as described above, from Inmediata's illegal disclosure and negligent release of their Personal and Medical Information in violation of Cal. Civ. Code §§ 56.10, 56.101, 56.26 and 56.36 and therefore seek relief under Civ. Code §§ 56.35 and 56.36, including actual damages, nominal statutory damages of $1,000, punitive damages of $3,000, injunctive relief, and attorney fees, expenses and costs.

282. As a direct and proximate result of Inmediata's violation of Cal. Civ. Code § 56 *et seq*., Plaintiffs and Class Members now face an increased risk of future harm.

283. As a direct and proximate result of Inmediata's violation of Cal. Civ. Code § 56 *et seq*., Plaintiffs and Class Members have suffered injury and are entitled to damages in an amount to be proven at trial.

284. Plaintiffs suffered a privacy injury by having their sensitive medical information disclosed, irrespective whether or not they subsequently suffered identity fraud, or incurred any mitigation damages. Medical information has been recognized as private sensitive information in common law and federal and state statutory schemes and the disclosure of such information resulted in cognizable injury to Plaintiffs.

COUNT V

VIOLATION OF CALIFORNIA'S CONSUMER PRIVACY ACT

Cal. Civ. Code § 1798.100 *et seq*.

285. Plaintiffs reallege and incorporate by reference every allegation set forth in the preceding paragraphs as though alleged in this Count.

286. This count is brought in the alternative to Plaintiffs' CMIA count.

287. This count is brought on behalf of the California Sub-Class.

288. Through the above-detailed conduct, Inmediata violated California's Consumer Privacy Act ("CCPA") by subjecting the nonencrypted and nonredacted Personal and Medical Information of Plaintiffs and Class Members to unauthorized access and exfiltration, theft, or disclosure as a result of Inmediata's violation of its duty to implement and maintain reasonable security procedures and practices appropriate to the nature and protection of that information. Cal. Civ. Code § 1798.150(a).

289. In accordance with Cal. Civ. Code §1798.150(b), prior to the filing of this Complaint, Plaintiffs' counsel served Inmediata with notice of these CCPA violations by certified mail, return receipt requested.

290. On behalf of Class Members, Plaintiffs seek injunctive relief in the form of an order enjoining Inmediata from continuing to violate the CCPA. If Inmediata fails to

respond to Plaintiffs' notice letter or agree to rectify the violations detailed above, Plaintiffs also will seek actual, punitive, and statutory damages, restitution, attorneys' fees and costs, and any other relief the Court deems proper as a result of Inmediata's CCPA violations.

COUNT VI

VIOLATION OF CALIFORNIA'S CONSUMER RECORDS ACT

Cal. Civ. Code § 1798.82 *et seq.*

291. Plaintiffs reallege and incorporate by reference every allegation set forth in the preceding paragraphs as though alleged in this Count.

292. This count is brought on behalf of all Classes.

293. Section 1798.2 of the California Civil Code requires any "person or business that conducts business in California, and that owns or licenses computerized data that includes personal information" to "disclose any breach of the security of the system following discovery or notification of the breach in the security of the data to any resident of California whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person." Under section 1798.82, the disclosure "shall be made in the most expedient time possible and without unreasonable delay . . . ."

294. The CCRA further provides: "Any person or business that maintains computerized data that includes personal information that the person or business does not own shall notify the owner or licensee of the information of any breach of the security of the data immediately following discovery, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person." Cal. Civ. Code § 1798.82(b).

295. Any person or business that is required to issue a security breach notification under the CCRA shall meet all of the following requirements:

a. The security breach notification shall be written in plain language;

b. The security breach notification shall include, at a minimum, the following information:

i. The name and contact information of the reporting person or business subject to this section;

ii. A list of the types of personal information that were or are reasonably believed to have been the subject of a breach;

iii. If the information is possible to determine at the time the notice is provided, then any of the following:

1. The date of the breach;

2. The estimated date of the breach; or

3. The date range within which the breach occurred. The notification shall also include the date of the notice.

iv. Whether notification was delayed as a result of a law enforcement investigation, if that information is possible to determine at the time the notice is provided;

v. A general description of the breach incident, if that information is possible to determine at the time the notice is provided; and

vi. The toll-free telephone numbers and addresses of the major credit reporting agencies if the breach exposed a Social Security number or a driver's license or California identification card number.

296. The Data Breach described herein constituted a "breach of the security system" of Inmediata.

297. As alleged above, by taking no less than 81 days to begin informing Plaintiffs and Class Members about the Data Breach, Inmediata unreasonably delayed informing Plaintiffs and Class Members about the Data Breach, affecting their Personal and Medical Information, after Inmediata knew the Data Breach had occurred.

298. Inmediata failed to disclose to Plaintiffs and Class Members, without unreasonable delay and in the most expedient time possible, the breach of security of their

unencrypted, or not properly and securely encrypted, Personal and Medical Information when Inmediata knew or reasonably believed such information had been compromised.

299. Inmediata's ongoing business interests gave Inmediata incentive to conceal the Data Breach from the public to ensure continued revenue.

300. Upon information and belief, no law enforcement agency instructed Inmediata that timely notification to Plaintiffs and Class Members would impede its investigation.

301. As a result of Inmediata's violation of Cal. Civ. Code § 1798.82, Plaintiffs and Class Members were deprived of prompt notice of the Data Breach and were thus prevented from taking appropriate protective measures, such as securing identity theft protection or requesting a credit freeze. These measures could have prevented some of the damages suffered by Plaintiffs and Class Members because their Personal and Medical Information would have had less value to identity thieves.

302. As a result of Inmediata' violation of Cal. Civ. Code § 1798.82, Plaintiffs and Class Members suffered incrementally increased damages separate and distinct from those simply caused by the Data Breach itself.

303. Plaintiffs and Class Members seek all remedies available under Cal. Civ. Code § 1798.84, including, but not limited to the damages suffered by Plaintiffs and Class Members as alleged above and equitable relief.

304. Inmediata's misconduct as alleged herein is fraud under Cal. Civ. Code § 3294(c)(3) in that it was deceit or concealment of a material fact known to the Inmediata conducted with the intent on the part of Inmediata of depriving Plaintiffs and Class Members of "legal rights or otherwise causing injury." In addition, Inmediata's misconduct as alleged herein is malice or oppression under Cal. Civ. Code § 3294(c)(1) and (c) in that it was despicable conduct carried on by Inmediata with a willful and conscious disregard of the rights or safety of Plaintiffs and Class Members and despicable conduct that has subjected Plaintiffs and Class Members to crewel and unjust hardship in

conscious disregard of their rights. As a result, Plaintiffs and Class Members are entitled to punitive damages against Inmediata under Cal. Civ. Code § 3294(a).

COUNT VII

VIOLATION OF THE MINNESOTA HEALTH RECORDS ACT

Minn. Stat. § 144.291 *et seq*.

305. Plaintiffs reallege and incorporate by reference every allegation set forth in the preceding paragraphs as though alleged in this Count.

306. This count is brought on behalf of the Minnesota Sub-Class.

307. Inmediata is a "Patient Information Service" as defined by Minn. Stat. § 144.291(Sub-2)(h), a "Provider" as defined by Minn. Stat. § 144.291(Sub-2)(i), and/or a "Related Health Care Entity" as defined by Minn. Stat. § 144.291(Sub-2)(k).

308. Plaintiffs and Class Members are "Patients" as defined by Minn. Stat. § 144.291(Sub-2)(g).

309. The Plaintiffs' and Class Members' Personal and Medical Information that was the subject of the Data Breach included "Health Records" as defined by Minn. Stat. § 144.291(Sub-2)(c).

310. The Plaintiffs' and Class Members' Personal and Medical Information that was the subject of the Data Breach included "Identifying Information" as defined by Minn. Stat. § 144.291(Sub-2)(d).

311. The Plaintiffs' and Class Members' Personal and Medical Information that was the subject of the Data Breach included information in an "Individually Identifiable Form" as defined by Minn. Stat. § 144.291(Sub-2)(e).

312. In violation of the Minnesota Health Records Act, Inmediata released Health Records of Plaintiffs and Class Members without first obtaining consent or authorization.

313. In violation of the Minnesota Health Records Act, Inmediata negligently or intentionally released Health Records of Plaintiffs and Class Members.

314. As a direct and proximate result of Inmediata's violation of Minn. Stat. §144.291 *et seq*., Plaintiffs and Class Members now face an increased risk of future harm.

315. As a direct and proximate result of Inmediata's violation of Minn. Stat. §144.291 *et seq*., Plaintiffs and Class Members have suffered injury and are entitled to damages in an amount to be proven at trial.

COUNT VIII

INVASION OF PRIVACY AND VIOLATION OF THE CALIFORNIA CONSTITUTION, ART. 1, § 1

316. Plaintiffs reallege and incorporate by reference every allegation set forth in the preceding paragraphs as though alleged in this Count.

317. This count is brought on behalf of all Classes.

318. Plaintiffs and Class Members had a reasonable expectation of privacy in the Personal and Medical Information that Defendant disclosed and/or accessed without authorization.

319. By failing to keep Plaintiffs' and Class Members' Personal and Medical Information safe, and by disclosing said information to unauthorized parties for unauthorized use, Defendant invaded Plaintiffs' and Class Members' privacy by, *inter alia*:

a. intruding into Plaintiffs' and Class Members' private affairs in a manner that would be highly offensive to a reasonable person; and

b. violating Plaintiffs' and Class Members' right to privacy under California Constitution, Article 1, Section 1, through the improper use of Plaintiffs' and Class Members' private information properly obtained for a specific purpose for another purpose, or the disclosure of it to some third party.

320. Defendant knew, or acted with reckless disregard of the fact that, a reasonable person in Plaintiffs' and Class Members' position would consider Defendant's actions highly offensive.

321. Defendant invaded Plaintiffs' and Class Members' right to privacy and intruded into Plaintiffs' and Class Members' private affairs by disclosing and/or

accessing their Personal and Medical Information without their informed, voluntary, affirmative, and clear consent.

322. As a proximate result of such unauthorized disclosures, Plaintiffs' and Class Members' reasonable expectations of privacy in their Personal and Medical Information was unduly frustrated and thwarted. Defendant's conduct amounted to a serious invasion of Plaintiffs' and Class Members' protected privacy interests.

323. In failing to protect Plaintiffs' and Class Members' Personal and Medical Information, and in disclosing Plaintiff's and Class Members' Personal and Medical Information, Defendant acted with malice and oppression and in conscious disregard of Plaintiffs' and Class Members' rights to have such information kept confidential and private.

324. Plaintiffs seek injunctive relief on behalf of the Classes, restitution, and all other damages available under this Count.

PRAYER FOR RELIEF

Plaintiffs, on behalf of themselves and the Classes, respectfully request the Court order relief and enter judgment in their favor and against Inmediata as follows:

A. An order certifying this action as a class action under Fed. R. Civ. P. 23, defining the Classes as requested herein, appointing the undersigned as Class counsel, and finding that Plaintiffs are proper representatives of the Classes requested herein.

B. Plaintiffs request injunctive and other equitable relief as is necessary to protect the interests of the Classes, including (i) an order prohibiting Inmediata from engaging in the wrongful and unlawful acts described herein; (ii) requiring Inmediata to protect all data collected or received through the course of their business in accordance with HIPAA regulations, the Gramm-Leach Bliley Act, other federal, state and local laws, and best practices under industry standards; (iii) requiring Inmediata to design, maintain, and test their computer systems to ensure that Personal and Medical Information in their possession is adequately secured and protected; (iv) requiring Inmediata to disclose any future data breaches in a timely and accurate manner; (v) requiring Inmediata to engage

third-party security auditors as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Inmediata's systems on a periodic basis and ordering them to promptly correct any problems or issues detected by these auditors; (vi) requiring Inmediata to audit, test, and train their security personnel to run automated security monitoring, aggregating, filtering and reporting on log information in a unified manner; (vii) requiring Inmediata to implement multi-factor authentication requirements; (viii) requiring Inmediata's employees to change their passwords on a timely and regular basis, consistent with best practices; (ix) requiring Inmediata to encrypt all Personal and Medical Information; (x) requiring Inmediata to audit, test, and train its security personnel regarding any new or modified procedures; (xi) requiring Inmediata to segment data by, among other things, creating firewalls and access controls so that if one area of Inmediata's network is compromised, hackers cannot gain access to other portions of Inmediata's systems; (xii) requiring Inmediata to purge, delete, and destroy in a reasonably secure and timely manner Personal and Medical Information no longer necessary for their provision of services; (xiii) requiring Inmediata to conduct regular database scanning and securing checks; (xiv) requiring Inmediata to 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; (xv) requiring Inmediata to provide lifetime credit monitoring and identity theft repair services to Class Members; and (xvi) requiring Inmediata to educate all Class Members about the threats they face as a result of the loss of their Personal and Medical Information to third parties, as well as steps Class Members must take to protect themselves.

C. A judgment awarding Plaintiffs and Class Members appropriate monetary relief, including actual damages, punitive damages, treble damages, statutory damages, exemplary damages, equitable relief, restitution, and disgorgement;

D. An order that Inmediata pay the costs involved in notifying the Class Members about the judgment and administering the claims process;

E. Pre-judgment and post-judgment interest;

F. Attorneys' fees, expenses, and the costs of this action; and

G. All other and further relief as this Court deems necessary, just, and proper.

JURY DEMAND

Plaintiffs demand a trial by jury on all issues so triable.

DATED: May 19, 2020

Respectfully submitted,

/s/ Tina Wolfson

Tina Wolfson
California Bar No. 174806
AHDOOT & WOLFSON, PC
10728 Lindbrook Drive
Los Angeles, CA 90024
Tel: 310.474.9111
Fax: 310.474.8585
twolfson@ahdootwolfson.com

and

Cornelius P. Dukelow*
Oklahoma Bar No. 19086
ABINGTON COLE + ELLERY
320 South Boston Avenue
Suite 1130
Tulsa, Oklahoma 74103
918.588.3400 (*telephone & facsimile*)
cdukelow@abingtonlaw.com

and

Benjamin F. Johns*
Pennsylvania Bar No. 201373
Andrew W. Ferich*
Pennsylvania Bar No. 313696
CHIMICLES SCHWARTZ KRINER
& DONALDSON-SMITH LLP
One Haverford Centre
361 Lancaster Avenue
Haverford, Pennsylvania 19041
610.642.8500
bfj@chimicles.com
awf@chimicles.com

**Pro Hac Vice*

Counsel to Plaintiffs and the Proposed Classes