Exhibit A

FILED
11th JUDICIAL DISTRICT COURT
McKinley County
6/4/2021 2:39 PM
WELDON J. NEFF
CLERK OF THE COURT
Jaycelyn Etsitty

STATE OF NEW MEXICO
COUNTY OF McKINLEY
ELEVENTH JUDICIAL DISTRICT

ALICIA CHARLIE, LEONA GARCIA LACY, DARRELL TSOSIE, and E.H., a minor, by and through his guardian, GARY HICKS *on behalf of themselves and a class of similarly situated individuals*,

PLAINTIFFS,

v.

Case No. D-1113-CV-2021-00235

REHOBOTH MCKINLEY CHRISTIAN HEALTH CARE SERVICES,

DEFENDANT.

CLASS ACTION COMPLAINT

Plaintiffs Alicia Charlie, Leona Garcia Lacy, Darrell Tsosie, and E.H., a minor, by and through his guardian Gary Hicks, individually and on behalf of all others similarly situated ("Plaintiffs"), bring this action against Defendant Rehoboth McKinley Christian Health Care Services ("RMCHCS") to obtain damages, restitution and injunctive relief for the Class, as defined below, from Defendant. Plaintiffs make the following allegations upon information and belief, except as to their own actions, the investigation of their counsel and certain facts that are a matter of public record.

NATURE OF THE ACTION

1. This class action lawsuit arises out of the recent targeted cyberattack and data breach on RMCHCS's network that resulted in unauthorized access and exfiltration of highly sensitive and personal patient data (the "Data Breach").

2. As a result of the Data Breach, Plaintiffs and approximately 207,191 Class Members[1] suffered ascertainable losses in the form of the loss of the benefit of their bargain, out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the unauthorized access and exfiltration of their sensitive and highly personal information.

3. In addition, Plaintiffs' and Class Members' sensitive personal information—which was entrusted to RMCHCS—was compromised and unlawfully accessed due to the Data Breach.

4. Information compromised in the Data Breach includes names, addresses, dates of birth, phone numbers, email addresses as well as Social Security, driver's license, passport and (for Native Americans) tribal identification numbers.[2]

5. Various healthcare-specific data as defined by the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), and additional personally identifiable information ("PII") and protected health information ("PHI") that Defendant RMCHCS collected and maintained (collectively, the "Private Information") was also involved, including, but not limited to, health insurance information, medical record numbers, dates of service and healthcare provider names, prescription, treatment and diagnosis information and billing and claims information, including financial account information.[3]

6. Plaintiffs bring this class action lawsuit on behalf of those similarly situated to address Defendant's inadequate safeguarding of Class Members' Private Information that they collected and maintained, and for failing to provide timely and adequate notice to Plaintiffs and

---

1 https://www.hipaajournal.com/rehoboth-mckinley-christian-health-care-services-notifies-patients-about-february-2021-ransomware-attack/ (last visited June 3, 2021).

2 https://portswigger.net/daily-swig/us-healthcare-non-profit-reports-data-breach-impacting-200-000-patients-employees (last visited June 3, 2021).

3 *Id.*

other Class Members that their information had been subject to the unauthorized access of a third party and precisely what specific type of information was accessed.

7. Upon information and belief, Defendant maintained the Private Information in a reckless manner. In particular, the Private Information was maintained on Defendant's computer system and network in a condition vulnerable to cyberattacks.

8. Upon information and belief, the mechanism of the cyberattack and potential for improper disclosure of Plaintiffs' and Class Members' Private Information was a known risk to Defendant,[4] and thus Defendant was on notice that failing to take steps necessary to secure the Private Information from those risks left that property in a dangerous condition.

9. Plaintiffs' and Class Members' identities are now at considerable risk because of Defendant's negligent conduct since the Private Information that RMCHCS collected and maintained is now in the hands of data thieves.

10. Armed with the Private Information accessed in the Data Breach, data thieves can commit a variety of crimes including, including, but not limited to, opening new financial accounts in Class Members' names, taking out loans in Class Members' names, using Class Members' names to obtain medical services, using Class Members' health information to target other phishing and hacking intrusions based on their individual health needs, using Class Members' information to obtain government benefits, filing fraudulent tax returns using Class Members' information, obtaining driver's licenses in Class Members' names but with another person's photograph and providing false information to police during an arrest.

11. As a result of the Data Breach, Plaintiffs and Class Members have been exposed to a heightened and imminent risk of fraud and identity theft. As a result of Defendant's actions and

---

[4] *See* https://www.rmch.org/getpage.php?name=medical_records (last visited June 3, 2021).

inactions, as set forth herein, Plaintiffs and Class Members must now and in the future closely monitor their financial and medical accounts and information to guard against identity theft, among other issues.

12. Plaintiffs and Class Members may also incur actual monetary costs, including, but not limited to, for purchasing credit monitoring services, credit freezes, credit reports or other protective measures to deter and detect identity theft.

13. By their Complaint, Plaintiffs seek to remedy these harms on behalf of themselves and all similarly situated individuals whose Private Information was accessed during the Data Breach.

14. Plaintiffs seek remedies including, but not limited to, compensatory damages, treble damages, punitive damages, reimbursement of out-of-pocket costs and injunctive relief including improvements to Defendant's data security systems, future annual audits and adequate credit monitoring services funded by Defendant.

15. Plaintiffs therefore bring this class action lawsuit against Defendant seeking redress for its unlawful conduct and asserting claims for: (i) negligence, (ii) intrusion into private affairs, (iii) negligence *per se*, (iv) breach of implied contract, (v) breach of fiduciary duty, (vi) unjust enrichment; (vii) violations of the New Mexico Unfair Practices Act, N.M. Stat. Ann. §§ 57-12-2, *et seq.* ("NMUPA") and (viii) violations of the Arizona Consumer Fraud Act, Ariz. Rev. Stat. §§ 44-1521, *et seq.* ("ACFA").

JURISDICTION AND VENUE

16. Jurisdiction and venue are proper in this Court pursuant to Article VI, § 13 of the New Mexico Constitution and NMSA 1978, § 38-3-1 (2006) because RMCHCS is located in

McKinley County, New Mexico and because many of the activities that gave rise to this claim occurred in this county.

17. This Court has personal jurisdiction over Defendant RMCHCS because Defendant is located in McKinley County, New Mexico, transacts business here, contracts to supply services here and caused tortious injury by act or omission within the State of New Mexico.

PARTIES

18. Plaintiff Alicia Charlie is, and at all times mentioned herein was, an individual citizen of the State of New Mexico.

19. Plaintiff Alicia Charlie was notified of the Data Breach and her Private Information being compromised upon receiving a data breach notice letter dated May 19, 2021.[5]

20. Plaintiff E.H., a minor, is, and at all times mentioned herein was, an individual citizen of the State of Arizona. E.H. brings this case by and through his guardian, Gary Hicks, an individual citizen of the State of Arizona.

21. Plaintiff E.H. was notified of the Data Breach upon receiving a data breach notice letter dated May 19, 2021.[6]

22. Plaintiff Leona Garcia Lacy is, and at all times mentioned herein was, an individual citizen of the State of New Mexico.

23. Plaintiff Leona Garcia Lacy was notified of the Data Breach and her Private Information being compromised upon receiving a data breach notice letter dated May 19, 2021.[7]

---

5 *See* Exhibit A.

6 *See* Exhibit B.

7 *See* Exhibit C.

24. Plaintiff Darrell Tsosie is, and at all times mentioned herein was, an individual citizen of the State of Arizona.

25. Plaintiff Darrell Tsosie was notified of the Data Breach and his Private Information being compromised upon receiving a data breach notice letter dated May 19, 2021.[8]

26. Defendant RMCHCS is a 501(c)(3) not-for-profit healthcare network located at 2111 College Drive in Gallup, New Mexico.[9]

DEFENDANT'S BUSINESS

27. RMCHCS offers a wide range of medical and diagnostic services and provides healthcare for people living in McKinley County and eastern Arizona.

28. RMCHCS operates a 60-bed acute care hospital, two outpatient clinics, home health, hospice and behavioral health services.

29. RMCHCS outpatient clinics offer acute primary care through its internal medicine and pediatrics practices and specialized services such as general surgery, obstetrics, gynecology, gerontology, infectious diseases and podiatry.

30. On information and belief, in the ordinary course of rendering healthcare care services, RMCHCS requires customers to provide personal and private information such as:

- Name, address, phone number and email address;
- Date of birth;
- Demographic information;
- Social Security number;
- Financial information;

---

8 *See* Exhibit D.

9 *See* https://www.rmch.org/getpage.php?name=about_us&sub=About%20Us

- Information relating to individual medical history;
- Information concerning an individual's health insurance plan or program;
- Information concerning an individual's doctor, nurse or other medical providers;
- Photo identification;
- Employment information and
- Other information that may be deemed necessary to provide care.

31. Additionally, RMCHCS may receive private and personal information from other individuals and/or organizations that are part of a customer's "circle of care," such as referring physicians, patients' other doctors, patients' health plan(s), close friends and/or family Members.

32. On information and belief, RMCHCS provides each of its customers with a HIPAA compliant notice (the "Privacy Notice") that explains how they handle customers' sensitive and confidential information.

33. Additionally, RMCHCS represents to the public and its customers, via its website, that it will safeguard and protect any confidential health and other personal information provided to it:

> Health information management is the collection of information pertaining to a patient who has been admitted, treated in the Emergency Department or Outpatient Care setting by a physician or other licensed authorized healthcare provider. The patient information that is collected during the visit is maintained in the Health Information Management or Medical Records Department. ***Health Information Management professionals are responsible for the collection, analysis, storage and protection of the quality of the patient's health information.*** The information collected can be paper-based, hybrid (combination of paper or digital) or a fully electronic health record (EHR).
>
> Health Information Management or Medical Records

> professionals work with physicians and other ancillary healthcare providers. ***They are responsible for ensuring that HIPAA laws that protect patient privacy, data analysis and how to harness computer systems that collect data are followed.*** They are also responsible for coding medical record data to ensure that the healthcare receives timely financial reimbursement for services rendered during a patient's encounter with the healthcare system.
>
> To summarize ***in short, Health Information Management or Medical Records is responsible for ensuring the availability, accuracy, and protection of the clinical information that is needed to deliver healthcare services and for the healthcare provider to be able to make appropriate healthcare-related decisions about a patient's treatment plan. They ensure that a patient's health information and records are complete, accurate, and protected.***[10]

34. Because of the highly sensitive and personal nature of the information it acquires and stores with respect to its patients, RMCHCS, upon information and belief, promises to, among other things: keep customers' protected health information (PHI) private; inform customers of its legal duties and comply with laws protecting customers' health information; only use and release customers' health information for approved reasons; provide adequate notice to customers if their Private Information is disclosed without authorization and adhere to the terms outlined in the Privacy Notice.[11]

35. As a condition of purchasing healthcare services from Defendant, RMCHCS requires that its customers entrust it with highly sensitive personal information.

36. By obtaining, collecting, using and deriving a benefit from Plaintiffs' and Class Members' Private Information, Defendant assumed legal and equitable duties and knew or should

---

[10] *See* https://www.rmch.org/getpage.php?name=medical_records (last visited June 3, 2021) (emphasis added).

[11] *Id.*

have known that it was responsible for protecting Plaintiffs' and Class Members' Private Information from unauthorized disclosure.

37. Plaintiffs and the Class Members have taken reasonable steps to maintain the confidentiality of their Private Information.

38. Plaintiffs and the Class Members relied on Defendant to keep their Private Information confidential and securely maintained, to use this information for business and health purposes only, and to make only authorized disclosures of this information.

THE CYBERATTACK AND DATA BREACH

39. According to RMCHCS, it became aware of a cybersecurity incident on February 16, 2021, which resulted in the Data Breach that exposed customers' Private Information.[12]

40. Specifically, and as set forth in its Notice of Data Breach letter, RMCHCS learned that "certain patient information may have been removed from [its] computer network as a result of potential unauthorized activity . . . ."[13]

41. That investigation revealed that an unauthorized actor "was able to access certain systems that contained patient information and remove some data between January 21 and February 5, 2021."[14]

42. The investigation further revealed that information accessed by the hackers included:

---

12 *See* https://ago.vermont.gov/blog/2021/05/19/rehoboth-mckinley-christian-health-care-services-notice-of-data-breach-to-consumers/ (last visited June 3, 2021).

13 *Id.*

14 https://response.idx.us/rmchcs/ (last visited June 3, 2021).

a. Information to identify and contact patients, including names, addresses, dates of birth, phone numbers and email addresses;

b. Social Security Numbers, driver's license numbers, passport numbers and/or tribal ID numbers;

c. health insurance information, such as names of insurer, plan numbers and member numbers;

d. medical information, such as Medical Record Numbers, dates of service, provider names, prescription information, treatment and diagnosis information and

e. billing and claims information including financial account information.[15]

43. The investigation revealed that approximately 207,195 individuals were victims of the Data Breach.[16]

44. The Data Breach remains under investigation by the U.S. Department of Health and Human Services' Office for Civil Rights.[17]

45. While RMCHCS stated in the "Notice of Data Breach" letter that it learned of the cybersecurity incident no later than February 16, 2021, it did not begin notifying victims until May 19, 2021 – *approximately three months after discovering the Data Breach.*

46. In that Notice letter posted on its website, RMCHCS openly admits that "certain patient information may have been removed from its computer network . . . ."[18]

---

15 *See id.*

16 *See* https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf (last visited June 3, 2021).

17 *See id.*

18 https://response.idx.us/rmchcs/ (last visited June 3, 2021).

47. This means that not only did the cybercriminals view and access the Private Information without authorization, but that they also removed Plaintiffs' and Class Members' Private Information from RMCHCS's computer network, and that it happened several months before Defendant got around to notifying its patients their Private Information is at risk.

48. Plaintiffs' Private Information was accessed and stolen in the Data Breach.

49. Plaintiffs further believe their Private Information was subsequently sold on the dark web following the Data Breach, as that is the typical *modus operandi* of all cybercriminals.

50. Defendant had obligations created by HIPAA, contract, industry standards, common law, and its own promises and representations made to Plaintiffs and Class Members to keep their Private Information confidential and to protect it from unauthorized access and disclosure.

51. Plaintiffs and Class Members provided their Private Information to Defendant with the reasonable expectation and mutual understanding that Defendant would comply with its obligations to keep such information confidential and secure from unauthorized access.

52. Defendant's data security obligations were particularly important given the substantial increase in cyberattacks and/or data breaches in the healthcare industry preceding the date of the breach.

53. In light of recent high profile data breaches at other healthcare partner and provider companies, including, American Medical Collection Agency (25 million patients, March 2019) University of Washington Medicine (974,000 patients, December 2018), Florida Orthopedic Institute (640,000 patients, July 2020), Wolverine Solutions Group (600,000 patients, September 2018), Oregon Department of Human Services (645,000 patients, March 2019), Elite Emergency Physicians (550,000 patients, June 2020), Magellan Health (365,000 patients, April 2020), BJC

Health System (286,876 patients, March 2020), Defendant knew or should have known that their electronic health records would be targeted by cybercriminals.

54. Indeed, cyberattacks have become so notorious that the FBI and U.S. Secret Service have issued a warning to potential targets so they are aware of, and prepared for, a potential attack.

55. As one report explained, "[e]ntities like smaller municipalities and hospitals are attractive. . . because they often have lesser IT defenses and a high incentive to regain access to their data quickly."[19]

56. In fact, according to the cybersecurity firm Mimecast, 90% of healthcare organizations experienced cyberattacks in the past year.[20]

57. Therefore, the increase in such attacks, and attendant risk of future attacks, was widely known to the public and to anyone in Defendant's industry, including Defendant.

Defendant Fails to Comply with FTC Guidelines

50. The Federal Trade Commission ("FTC") has promulgated numerous guides for businesses which highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.

51. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established cyber-security guidelines for businesses. These guidelines note that businesses should protect the personal customer information that they keep; properly

---

[19] *FBI, Secret Service Warn of Targeted*, Law360 (Nov. 18, 2019), https://www.law360.com/articles/1220974/fbi-secret-service-warn-of-targeted-ransomware (last visited June 3, 2021).

[20] *See* Maria Henriquez, Iowa City Hospital Suffers Phishing Attack, Security Magazine (Nov. 23, 2020), https://www.securitymagazine.com/articles/93988-iowa-city-hospital-suffers-phishing-attack.

dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct any security problems.[21]

52. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.[22]

53. The FTC further recommends that companies not maintain PII longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.

54. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

55. These FTC enforcement actions include actions against healthcare providers like Defendant. *See, e.g., In the Matter of Labmd, Inc., A Corp*, 2016-2 Trade Cas. (CCH) ¶ 79708,

---

[21] *Protecting Personal Information: A Guide for Business*, Federal Trade Commission (2016). Available at https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last visited June 3, 2021).

[22] *Id.*

2016 WL 4128215, at *32 (MSNET July 28, 2016) ("[T]he Commission concludes that LabMD's data security practices were unreasonable and constitute an unfair act or practice in violation of Section 5 of the FTC Act.")

56. Defendant failed to properly implement basic data security practices.

57. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to customers' PII and PHI constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

58. Upon information and belief, Defendant was at all times fully aware of its obligation to protect the PII and PHI of their customers. Defendant was also aware of the significant repercussions that would result from its failure to do so.

Defendant Fails to Comply with Industry Standards

59. As noted above, experts studying cyber security routinely identify healthcare providers as being particularly vulnerable to cyberattacks because of the value of the PII and PHI which they collect and maintain.

60. Several best practices have been identified that a minimum should be implemented by healthcare providers like Defendant, including but not limited to: educating all employees; strong passwords; multi-layer security, including firewalls, anti-virus, and anti-malware software; encryption, making data unreadable without a key; multi-factor authentication; backup data and limiting which employees can access sensitive data.

61. Other best cybersecurity practices that are standard in the healthcare industry include installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches and routers; monitoring and protection of physical security systems;

protection against any possible communication system; training staff regarding critical points.

62. Defendant failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

63. These foregoing frameworks are existing and applicable industry standards in the healthcare industry, and Defendant failed to comply with these accepted standards thereby opening the door to the cyber incident and causing the data breach.

Defendant's Conduct Violates HIPAA and Evidences Its Insufficient Data Security

64. HIPAA requires covered entities to protect against reasonably anticipated threats to the security of sensitive patient health information.

65. Covered entities must implement safeguards to ensure the confidentiality, integrity, and availability of PHI. Safeguards must include physical, technical and administrative components.

66. Title II of HIPAA contains what are known as the Administrative Simplification provisions. 42 U.S.C. §§ 1301, *et seq.* These provisions require, among other things, that the Department of Health and Human Services ("HHS") create rules to streamline the standards for handling PII like the data Defendant left unguarded. The HHS subsequently promulgated multiple regulations under authority of the Administrative Simplification provisions of HIPAA. These rules include 45 C.F.R. § 164.306(a)(1-4); 45 C.F.R. § 164.312(a)(1); 45 C.F.R. § 164.308(a)(1)(i); 45 C.F.R. § 164.308(a)(1)(ii)(D), and 45 C.F.R. § 164.530(b).

67. A Data Breach such as the one Defendant experienced, is considered a breach under the HIPAA Rules because there is an access of PHI not permitted under the HIPAA Privacy Rule:

> A breach under the HIPAA Rules is defined as, "...the acquisition, access, use, or disclosure of PHI in a manner not permitted under the [HIPAA Privacy Rule] which compromises the security or privacy of the PHI."[23]

68. Defendant's Data Breach resulted from a combination of insufficiencies that demonstrate RMCHCS failed to comply with safeguards mandated by HIPAA regulations.

DEFENDANT'S BREACH

69. Defendant breached its obligations to Plaintiffs and Class Members and/or was otherwise negligent and reckless because it failed to properly maintain and safeguard its computer systems and data.

70. Defendant's unlawful conduct includes, but is not limited to, the following acts and/or omissions:

a. Failing to maintain an adequate data security system to reduce the risk of data breaches and cyber-attacks;

b. Failing to adequately protect customers' Private Information;

c. Failing to properly monitor its own data security systems for existing intrusions;

d. Failing to ensure that its vendors with access to its computer systems and data employed reasonable security procedures;

e. Failing to train its employees in the proper handling of emails containing PII and PHI and maintain adequate email security practices;

---

[23] *See* 45 C.F.R. § 164.40.

f. Failing to ensure the confidentiality and integrity of electronic PHI it created, received, maintained, and/or transmitted, in violation of 45 C.F.R. § 164.306(a)(1);

g. Failing to implement technical policies and procedures for electronic information systems that maintain electronic PHI 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);

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

i. Failing to implement 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);

j. Failing to protect against reasonably anticipated threats or hazards to the security or integrity of electronic PHI in violation of 45 C.F.R. § 164.306(a)(2);

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

l. Failing to ensure compliance with HIPAA security standard rules by its workforces in violation of 45 C.F.R. § 164.306(a)(4);

m. Failing to train all members of its workforces effectively on the policies and procedures regarding PHI as necessary and appropriate for the members of

its workforces to carry out their functions and to maintain security of PHI, in violation of 45 C.F.R. § 164.530(b);

n. Failing to render the electronic PHI it maintained unusable, unreadable, or indecipherable to unauthorized individuals, as it had not encrypted the electronic PHI as specified in the HIPAA Security Rule by "the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key" (45 CFR § 164.304's definition of "encryption");

o. Failing to comply with FTC guidelines for cybersecurity, in violation of Section 5 of the FTC Act, and;

p. Failing to adhere to industry standards for cybersecurity.

71. Defendant negligently and unlawfully failed to safeguard Plaintiffs' and Class Members' Private Information by allowing cyberthieves to access RMCHCS's computer network and systems which contained unsecured and unencrypted PII.

72. Accordingly, as outlined below, Plaintiffs and Class Members now face an increased risk of fraud and identity theft. In addition, Plaintiffs and the Class Members also lost the benefit of the bargain they made with Defendant.

Cyberattacks and Data Breaches Cause Disruption and Put Consumers at an Increased Risk of Fraud and Identity Theft

73. Cyberattacks and data breaches at healthcare providers like Defendant are especially problematic because they can negatively impact the overall daily lives of individuals affected by the attack.

74. Researchers have found that among medical service providers that experience a data security incident, the death rate among patients increased in the months and years after the

attack.[24]

75. Researchers have further found that at medical service providers that experienced a data security incident, the incident was associated with deterioration in timeliness and patient outcomes, generally.[25]

76. The United States Government Accountability Office released a report in 2007 regarding data breaches ("GAO Report") in which it noted that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."[26]

77. That is because any victim of a data breach is exposed to serious ramifications regardless of the nature of the data. Indeed, the reason criminals steal personally identifiable information is to monetize it. They do this by selling the spoils of their cyberattacks on the black market to identity thieves who desire to extort and harass victims, take over victims' identities in order to engage in illegal financial transactions under the victims' names.

78. Because a person's identity is akin to a puzzle, the more accurate pieces of data an identity thief obtains about a person, the easier it is for the thief to take on the victim's identity or otherwise harass or track the victim. For example, armed with just a name and date of birth, a data thief can utilize a hacking technique referred to as "social engineering" to obtain even more information about a victim's identity, such as a person's login credentials or Social Security number. Social engineering is a form of hacking whereby a data thief uses previously acquired

---

[24] *See* Nsikan Akpan, *Ransomware and Data Breaches Linked to Uptick in Fatal Heart Attacks*, PBS (Oct. 24, 2019), https://www.pbs.org/newshour/science/ransomware-and-other-data-breaches-linked-to-uptick-in-fatal-heart-attacks.

[25] *See* Sung J. Choi, *et al.*, *Data Breach Remediation Efforts and Their Implications for Hospital Quality*, 54 Health Services Research 971, 971-980 (2019). Available at https://onlinelibrary.wiley.com/doi/full/10.1111/1475-6773.13203.

[26] *See* U.S. Gov. Accounting Office, GAO-07-737, Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown (2007). Available at https://www.gao.gov/new.items/d07737.pdf.

information to manipulate individuals into disclosing additional confidential or personal information through means such as spam phone calls and text messages or phishing emails.

79. The FTC recommends that identity theft victims take several steps to protect their personal and financial information after a data breach, including contacting one of the credit bureaus to place a fraud alert (consider an extended fraud alert that lasts for 7 years if someone steals their identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit and correcting their credit reports.[27]

80. Identity thieves use stolen personal information such as Social Security numbers for a variety of crimes, including credit card fraud, phone or utilities fraud and bank/finance fraud.

81. Identity thieves can also use Social Security numbers to obtain a driver's license or official identification card in the victim's name but with the thief's picture; use the victim's name and Social Security number to obtain government benefits or file a fraudulent tax return using the victim's information.

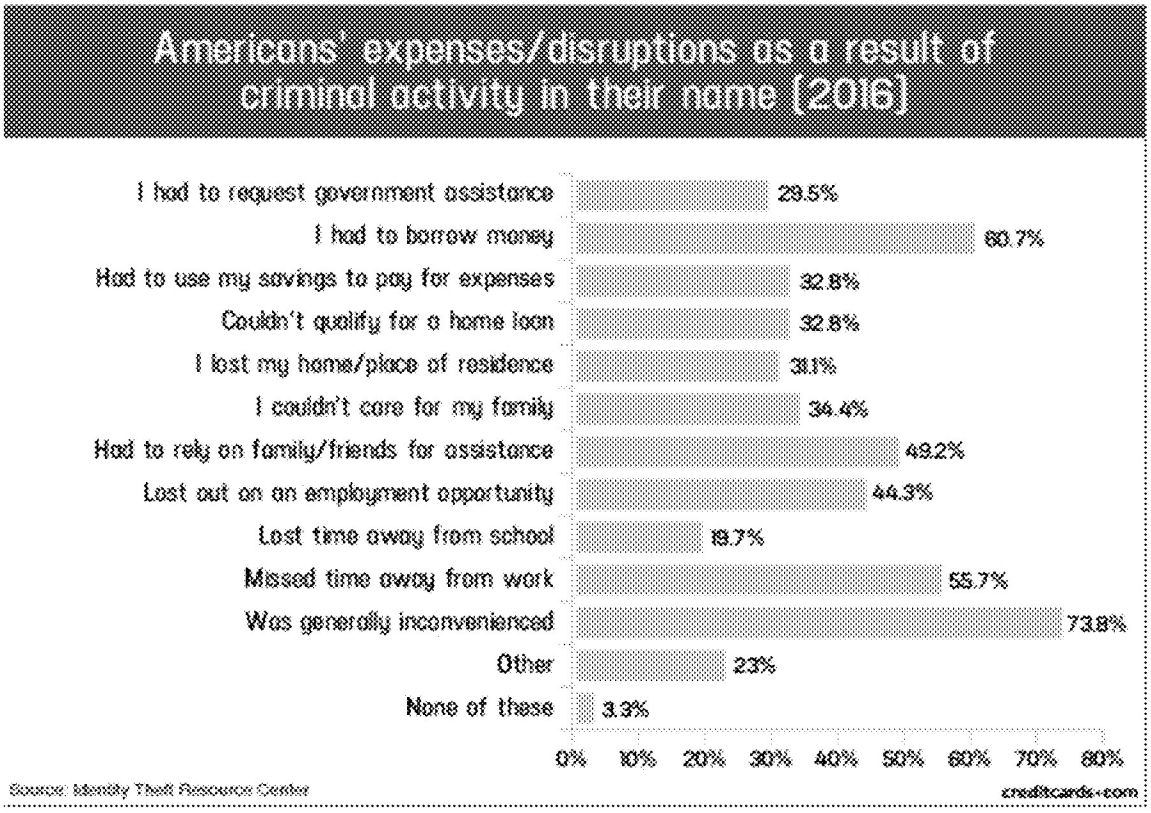
82. In addition, identity thieves may obtain a job using the victim's Social Security number, rent a house or receive medical services in the victim's name, and may even give the victim's personal information to police during an arrest resulting in an arrest warrant being issued in the victim's name.

83. A study by Identity Theft Resource Center shows the multitude of harms caused by fraudulent use of personal and financial information:[28]

---

[27] *See IdentityTheft.gov*, Federal Trade Commission, https://www.identitytheft.gov/Steps (last visited June 3, 2021).

[28] *See* Jason Steele, *Credit Card and ID Theft Statistics*, CreditCards.com (Oct. 23, 2020) https://www.creditcards.com/credit-card-news/credit-card-security-id-theft-fraud-statistics-1276.php.



84. Moreover, theft of Private Information is gravely serious; PII and PHI is an extremely valuable property right.[29]

85. Its value is axiomatic, considering the value of "big data" in corporate America and the fact that the consequences of cyber thefts include heavy prison sentences. Even this obvious risk to reward analysis illustrates beyond doubt that Private Information has considerable market value.

86. Theft of PHI, in particular, is gravely serious: "[a] thief may use your name or health insurance numbers to see a doctor, get prescription drugs, file claims with your insurance provider, or get other care. If the thief's health information is mixed with yours, your treatment,

[29] *See, e.g.*, John T. Soma, *et al*, *Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("PII") Equals the "Value" of Financial Assets*, 15 Rich. J.L. & Tech. 11, at *3-4 (2009) ("PII, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets.") (citations omitted).

insurance and payment records, and credit report may be affected."[30]

87. Drug manufacturers, medical device manufacturers, pharmacies, hospitals and other healthcare service providers often purchase PII and PHI on the black market for the purpose of target marketing their products and services to the physical maladies of the data breach victims themselves. Insurance companies purchase and use wrongfully disclosed PHI to adjust their insureds' medical insurance premiums.

88. Compounding issues for data breach victims is the fact that there may be a substantial time lag – measured in years – between when harm occurs and when it is discovered and also between when Private Information and/or financial information is stolen and when it is used.

89. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches:

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

See GAO Report, at 29.

90. Private 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.

91. There is a strong probability that entire batches of stolen information have been dumped on the black market and are yet to be dumped on the black market, meaning Plaintiffs and

---

[30] *See* Federal Trade Commission, *Medical Identity Theft*, http://www.consumer.ftc.gov/articles/0171-medical-identity-theft (last visited June 3, 2021).

Class Members are at an increased risk of fraud and identity theft for many years into the future.

92. Thus, Plaintiffs and Class Members must vigilantly monitor their financial and medical accounts for many years to come.

93. Sensitive Private Information can sell for as much as $363 per record according to the Infosec Institute.[31]

94. PII is particularly valuable because criminals can use it to target victims with frauds and scams. Once PII is stolen, fraudulent use of that information and damage to victims may continue for years.

95. For example, the Social Security Administration has warned that identity thieves can use an individual's Social Security number to apply for additional credit lines.[32] Such fraud may go undetected until debt collection calls commence months, or even years, later.

96. Stolen Social Security Numbers also make it possible for thieves to file fraudulent tax returns, file for unemployment benefits, or apply for a job using a false identity.[33]

97. Each of these fraudulent activities is difficult to detect. An individual may not know that his or her Social Security Number was used to file for unemployment benefits until law enforcement notifies the individual's employer of the suspected fraud. Fraudulent tax returns are typically discovered only when an individual's authentic tax return is rejected.

98. Moreover, it is not an easy task to change or cancel a stolen Social Security number.

99. An individual cannot obtain a new Social Security number without significant

---

31 *See* Ashiq Ja, *Hackers Selling Healthcare Data in the Black Market*, InfoSec (July 27, 2015), https://resources.infosecinstitute.com/topic/hackers-selling-healthcare-data-in-the-black-market/.

32 *Identity Theft and Your Social Security Number*, Social Security Administration (2018) at 1. Available at https://www.ssa.gov/pubs/EN-05-10064.pdf (last visited June 3, 2021).

33 *Id.* at 4.

paperwork and evidence of actual misuse. Even then, a new Social Security number may not be effective, as "[t]he credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[34]

100. This data, as one would expect, demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "[c]ompared to credit card information, personally identifiable information and Social Security Numbers are worth more than 10x on the black market."[35]

101. Medical information is especially valuable to identity thieves.

102. According to account monitoring company LogDog, coveted Social Security numbers were selling on the dark web for just $1 in 2016 – the same as a Facebook account.[36] That pales in comparison with the asking price for medical data, which was selling for $50 and up.[37]

103. Because of the value of its collected and stored data, the medical industry has experienced disproportionally higher numbers of data theft events than other industries.

104. For this reason, Defendant knew or should have known about these dangers and strengthened its data and email handling systems accordingly. Defendant was put on notice of the

---

[34] Brian Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR (Feb. 9, 2015), http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millions-worrying-about-identity-theft.

[35] Tim Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, Computer World (Feb. 6, 2015), http://www.itworld.com/article/2880960/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html.

[36] *See* Omri Toppol, *Email Security: How You Are Doing It Wrong & Paying Too Much*, LogDog (Feb. 14, 2016), https://getlogdog.com/blogdog/email-security-you-are-doing-it-wrong/.

[37] Lisa Vaas, *Ransomware Attacks Paralyze, and Sometimes Crush, Hospitals*, Naked Security (Oct. 3, 2019), https://nakedsecurity.sophos.com/2019/10/03/ransomware-attacks-paralyze-and-sometimes-crush-hospitals/#content.

substantial and foreseeable risk of harm from a data breach, yet RMCHCS failed to properly prepare for that risk.

Plaintiffs' and Class Members' Damages

105. To date, Defendant has done little to nothing to provide Plaintiffs and the Class Members with relief for the damages they have suffered as a result of the Data Breach.

106. Defendant has merely offered Plaintiffs and Class Members complimentary fraud and identity monitoring services for up to twelve (12) months, but this does nothing to compensate them for damages incurred and time spent dealing with the Data Breach.[38]

107. Plaintiffs and Class Members have been damaged by the compromise of their Private Information in the Data Breach.

108. Plaintiffs' names, addresses, dates of birth, phone numbers, Social Security Numbers, medical diagnosis, insurance information and other protected health information were all compromised in the Data Breach and are now in the hands of the cybercriminals who accessed Defendant's computer system.

109. As a result of the Data Breach, Plaintiff Alicia Charlie has experienced a substantial increase in suspicious scam phone calls which appear to be placed with the intent to obtain personal information to commit identity theft by way of a social engineering attack.

110. Since being notified of the Data Breach, Plaintiff Alicia Charlie has been monitoring her accounts for fraud and dealing with the impact of the Data Breach at least three times per week, valuable time Plaintiff otherwise would have spent on other activities.

111. As a result of the Data Breach, Plaintiff E.H. received a notice letter regarding the

---

[38] *See* Ex. A, Notice Letter at 2 (stating that "[b]ecause it is possible that your Social Security number or financial account information may have been involved, we have arranged to offer you credit monitoring and identity restoration services for a period of 12 months, at no cost to you through an identity and privacy protection company named IDX").

unauthorized access and breach of his confidential health information, and consequently his guardian, Gary Hicks, has to expend time and resources dealing with the impact of the Data Breach, valuable time Plaintiff otherwise would have spent on other activities.

112. As a result of the Data Breach, Plaintiff Leona Garcia Lacy has begun to receive phishing calls regarding a payday loan (wherein the caller uses Plaintiff's prior name, which was used by RMCHCS). Such suspicious scam phone calls are often placed with the intent to obtain personal information, including financial information, to commit fraud and/or identity theft.

113. Since being notified of the Data Breach, Plaintiff Leona Garcia Lacy has spent at least 2 hours per week monitoring her accounts for fraud and dealing with the impact of the Data Breach, valuable time Plaintiff otherwise would have spent on other activities.

114. As a result of the Data Breach, Plaintiff Darrell Tsosie received a notice letter regarding the unauthorized access and breach of his confidential health information, and consequently he has to expend time and resources dealing with the impact of the Data Breach, valuable time Plaintiff otherwise would have spent on other activities.

115. Due to the Data Breach, Plaintiffs anticipate spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach.

116. Plaintiffs' Private Information was compromised as a direct and proximate result of the Data Breach.

117. As a direct and proximate result of Defendant's conduct, Plaintiffs and Class Members have been placed at an imminent, immediate and continuing increased risk of harm from fraud and identity theft.

118. As a direct and proximate result of Defendant's conduct, Plaintiffs and Class Members have been forced to expend time dealing with the effects of the Data Breach.

119. Plaintiffs and Class Members face substantial risk of out-of-pocket fraud losses such as loans opened in their names, medical services billed in their names, tax return fraud, utility bills opened in their names, credit card fraud and similar identity theft.

120. Plaintiffs and Class Members face substantial risk of being targeted for future phishing, data intrusion, and other illegal schemes based on their Private Information as potential fraudsters could use that information to more effectively target such schemes to Plaintiffs and Class Members.

121. Plaintiffs and Class Members may also incur out-of-pocket costs for protective measures such as credit monitoring fees (after expiration of the 12 month period offered by Defendant), credit report fees, credit freeze fees and similar costs directly or indirectly related to the Data Breach.

122. Plaintiffs and Class Members also suffered a loss of value of their Private Information when it was acquired by cyber thieves in the Data Breach. Numerous courts have recognized the propriety of loss of value damages in related cases.

123. Plaintiffs and Class Members were also damaged via benefit-of-the-bargain damages. Plaintiffs and Class Members overpaid for a service that was intended to be accompanied by adequate data security but was not. Part of the price Plaintiffs and Class Members paid to Defendant was intended to be used by Defendant to fund adequate security of RMCHCS's computer property and Plaintiffs' and Class Members' Private Information. Thus, Plaintiffs and the Class Members did not get what they paid for and agreed to.

124. Plaintiffs and Class Members have spent and will continue to spend significant amounts of time to monitor their medical accounts and sensitive information for misuse.

125. Plaintiffs and Class Members have suffered or will suffer actual injury as a direct

result of the Data Breach. Many victims suffered ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach relating to:

a. Reviewing and monitoring sensitive accounts and finding fraudulent insurance claims, loans, and/or government benefits claims;

b. Purchasing credit monitoring and identity theft prevention;

c. Placing "freezes" and "alerts" with reporting agencies;

d. Spending time on the phone with or at financial institutions, healthcare providers, and/or government agencies to dispute unauthorized and fraudulent activity in their name;

e. Contacting financial institutions and closing or modifying financial accounts; and,

f. Closely reviewing and monitoring Social Security Number, medical insurance accounts, bank accounts, and credit reports for unauthorized activity for years to come.

126. Moreover, Plaintiffs and Class Members have an interest in ensuring that their Private Information, which is believed to remain in the possession of Defendant, is protected from further breaches by the implementation of security measures and safeguards, including but not limited to, making sure that the storage of data or documents containing Private Information is not accessible online and that access to such data is password protected.

127. Further, as a result of Defendant's conduct, Plaintiffs and Class Members are forced to live with the anxiety that their Private Information—which contains the most intimate details about a person's life, including what ailments they suffer, whether physical or mental—may be

disclosed to the entire world, thereby subjecting them to embarrassment and depriving them of any right to privacy whatsoever.

128. As a direct and proximate result of Defendant's actions and inactions, Plaintiffs and Class Members have suffered anxiety, emotional distress, and loss of privacy, and are at an increased risk of future harm.

CLASS ACTION ALLEGATIONS

129. Plaintiffs bring this action on behalf of themselves and on behalf of all other persons similarly situated.

130. Plaintiffs propose the following Class definitions, subject to amendment as appropriate:

> All persons RMCHCS identified as being among those individuals impacted by the Data Breach, including all who were sent a notice of the Data Breach (the "Class").
>
> All patients and/or customers RMCHCS identified as being among those individuals impacted by the Data Breach, including all who were sent a notice of the Data Breach (the "Customer Sub-class").
>
> All patients and/or customers residing in New Mexico RMCHCS identified as being among those individuals impacted by the Data Breach, including all who were sent a notice of the Data Breach (the "New Mexico Customer Sub-class").
>
> All patients and/or customers residing in Arizona RMCHCS identified as being among those individuals impacted by the Data Breach, including all who were sent a notice of the Data Breach (the "Arizona Customer Sub-class").

131. Excluded from the Class' are Defendant's officers, directors, and employees; any entity in which Defendant has a controlling interest; and the affiliates, legal representatives, attorneys, successors, heirs, and assigns of Defendant. Excluded also from the Class are members of the judiciary to whom this case is assigned, their families and Members of their staff.

132. Numerosity. The Members of the Class' are so numerous that joinder of all of them is impracticable. While the exact number of Class Members is unknown to Plaintiff at this time, based on information and belief, the Class consists of approximately 207,195 consumers of RMCHCS whose sensitive data was compromised in Data Breach.[39]

133. Commonality. There are questions of law and fact common to the Class, which predominate over any questions affecting only individual Class Members. These common questions of law and fact include, without limitation:

a. Whether Defendant unlawfully used, maintained, lost, or disclosed Plaintiffs' and Class Members' Private Information;

b. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

c. Whether Defendant's data security systems prior to and during the Data Breach complied with applicable data security laws and regulations including, *e.g.*, HIPAA;

d. Whether Defendant's data security systems prior to and during the Data Breach were consistent with industry standards;

e. Whether Defendant owed a duty to Class Members to safeguard their Private Information;

f. Whether Defendant breached its duty to Class Members to safeguard their Private Information;

[39] https://portswigger.net/daily-swig/us-healthcare-non-profit-reports-data-breach-impacting-200-000-patients-employees (last visited June 3, 2021).

g. Whether Defendant knew or should have known that its data security systems and monitoring processes were deficient;

h. Whether Defendant should have discovered the Data Breach sooner;

i. Whether Plaintiffs and Class Members suffered legally cognizable damages as a result of Defendant's misconduct;

j. Whether Defendant's conduct was negligent;

k. Whether Defendant's acts, inactions and practices complained of herein amount to acts of intrusion upon seclusion under the law;

l. Whether Defendant breached a fiduciary duty to Plaintiffs and Class Members;

m. Whether Defendant violated the consumer protection statute invoked below;

n. Whether Defendant breach implied or express contracts with Plaintiffs and Class Members;

o. Whether Defendant was unjustly enriched by unlawfully retaining a benefit conferred upon them by Plaintiffs and Class Members;

p. Whether Defendant failed to provide notice of the Data Breach in a timely manner, and;

q. Whether Plaintiffs and Class Members are entitled to damages, civil penalties, punitive damages, treble damages, and/or injunctive relief.

134. Typicality. Plaintiffs' claims are typical of those of other Class Members because Plaintiffs' information, like that of every other Class Member, was compromised in the Data

Breach.

135. Adequacy of Representation. Plaintiffs will fairly and adequately represent and protect the interests of the Members of the Class'. Plaintiffs' Counsel are competent and experienced in litigating Class actions.

136. Predominance. Defendant have engaged in a common course of conduct toward Plaintiffs and Class Members, in that all the Plaintiffs' and Class Members' data was stored on the same computer system and unlawfully accessed in the same way. The common issues arising from Defendant's conduct affecting Class Members set out above predominate over any individualized issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

137. Superiority. A Class action is superior to other available methods for the fair and efficient adjudication of the controversy. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a Class action, most Class Members would likely find that the cost of litigating their individual claims is prohibitively high and would therefore have no effective remedy. The prosecution of separate actions by individual Class Members would create a risk of inconsistent or varying adjudications with respect to individual Class Members, which would establish incompatible standards of conduct for Defendant. In contrast, the conduct of this action as a Class action presents far fewer management difficulties, conserves judicial resources and the parties' resources, and protects the rights of each Class Member.

138. Defendant has acted on grounds that apply generally to the Class as a whole, so that Class certification, injunctive relief, and corresponding declaratory relief are appropriate on a Class-wide basis.

CAUSES OF ACTION
FIRST COUNT

NEGLIGENCE

(On Behalf of Plaintiffs & the Class)

139. Plaintiffs re-allege and incorporate by reference Paragraphs 1 through 138 above as if fully set forth herein.

140. Defendant required customers, including Plaintiffs and Class Members, to submit non-public Private Information in the ordinary course of rendering healthcare services.

141. By collecting and storing this data in its computer property, and sharing it and using it for commercial gain, Defendant owed a duty of care to use reasonable means to secure and safeguard its computer property—and Class Members' Private Information held within it—to prevent disclosure of the information, and to safeguard the information from unauthorized access and exfiltration.

142. Defendant's duty included a responsibility to implement processes by which they could detect a breach of its security systems in a reasonably expeditious period of time and to give prompt notice to those affected in the case of a data breach.

143. Defendant owed a duty of care to Plaintiffs and Class Members to provide data security consistent with industry standards and other requirements discussed herein, and to ensure that its systems and networks (and the personnel responsible for them) adequately protected the Private Information.

144. Defendant's duty of care to use reasonable security measures arose as a result of the special relationship that existed between Defendant and its customers, which is recognized by laws and regulations including but not limited to HIPAA, as well as common law.

145. Defendant was in a superior position to ensure that its systems were sufficient to

protect against the foreseeable risk of harm to Class Members from a data breach.

146. Defendant's duty to use reasonable security measures under HIPAA required Defendant to "reasonably protect" confidential data from "any intentional or unintentional use or disclosure" and to "have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information." 45 C.F.R. § 164.530(c)(1).

147. Some or all of the medical information at issue in this case constitutes "protected health information" within the meaning of HIPAA.

148. In addition, Defendant had a duty to employ reasonable security measures under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data.

149. Defendant's duty to use reasonable care in protecting confidential data arose not only as a result of the statutes and regulations described above, but also because Defendant is bound by industry standards to protect confidential Private Information.

150. Defendant breached its duties, and thus was negligent, by failing to use reasonable measures to protect Class Members' Private Information. The specific negligent acts and omissions committed by Defendant include, but are not limited to, the following:

a. Failing to adopt, implement and maintain adequate security measures to safeguard Class Members' Private Information;

b. Failing to adequately monitor the security of their networks and systems;

c. Failing to ensure that their email system had plans in place to maintain reasonable data security safeguards;

d. Failing to have in place mitigation policies and procedures;

e. Allowing unauthorized access to Class Members' Private Information;

f. Failing to detect in a timely manner that Class Members' Private Information had been compromised; and

g. Failing to timely notify Class Members about the Data Breach so that they could take appropriate steps to mitigate the potential for identity theft and other damages.

151. It was foreseeable that Defendant's failure to use reasonable measures to protect Class Members' Private Information would result in injury to Class Members.

152. Further, the breach of security was reasonably foreseeable given the known high frequency of cyberattacks and data breaches in the healthcare industry.

153. It was therefore foreseeable that the failure to adequately safeguard Class Members' Private Information would result in one or more types of injuries to Class Members.

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

155. Plaintiffs and Class Members are also entitled to injunctive relief requiring Defendant to, *e.g.*, (i) strengthen their data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures and (iii) continue to provide adequate credit monitoring to all Class Members.

SECOND COUNT

INTRUSION UPON SECLUSION / INVASION OF PRIVACY

(On Behalf of Plaintiffs and the Customer Sub-Classes)

156. Plaintiffs repeat and re-allege each and every allegation contained in Paragraphs 1 through 155 as if fully set forth herein.

157. The State of New Mexico recognizes the tort of invasion of the right of privacy. Plaintiff and Class Members had a reasonable expectation of privacy in the Private Information Defendant failed to protect as warranted.

158. One who intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns, is subject to liability to the other for invasion of his privacy, if the intrusion would be highly offensive to a reasonable person.

159. Plaintiffs and Class Members had a reasonable expectation of privacy in the Private Information Defendant failed to protect as warranted.

160. Defendant's conduct as alleged above intruded upon Plaintiffs' and Class Members' seclusion and privacy under common law.

161. By intentionally failing to keep Plaintiffs' and Class Members' Private Information safe, and by intentionally misusing and/or disclosing said information to unauthorized parties for unauthorized use, Defendant intentionally invaded Plaintiffs' and Class Members' privacy by:

a. Intentionally and substantially intruding into Plaintiffs' and Class Members' private affairs, without approval, in a manner that identifies

Plaintiffs and Class Members and that would be highly offensive and objectionable to a person of ordinary sensibilities;

b. Intentionally publicizing private facts about Plaintiffs and Class Members, which is highly offensive and objectionable to a person with ordinary sensibilities and

c. Intentionally causing anguish or suffering to Plaintiff and Class Members.

162. Defendant knew that an ordinary person in Plaintiffs' or a Class Member's position would consider Defendant's intentional actions highly offensive and objectionable.

163. Such an intrusion into Plaintiffs' private affairs is likely to cause outrage, shame, and mental suffering because the Private Information disclosed is medical and health information that details medical conditions Plaintiffs suffer from and the medical assistance required, information that is only shared with others when an individual is comfortable.

164. Defendant invaded Plaintiffs and Class Members' right to privacy and intruded into Plaintiffs' and Class Members' private life by intentionally misusing and/or disclosing their Private Information without their informed, voluntary, affirmative and clear consent.

165. The Private Information disclosed by Defendant, Plaintiffs' and Class Members' PHI and other Private Information, has no legitimate reason to be known by the public.

166. Defendant intentionally concealed from Plaintiffs and Class Members an incident that misused and/or disclosed their Private information without their informed, voluntary, affirmative, and clear consent.

167. As a proximate result of such intentional misuse and disclosures, Plaintiffs' and Class Members' reasonable expectations of privacy in their Private Information was unduly frustrated and thwarted.

168. Defendant's conduct, amounting to a substantial and serious invasion of Plaintiffs' and Class Members' protected privacy interests causing anguish and suffering such that a person with ordinary sensibilities would consider Defendant's intentional actions or inaction highly offensive and objectionable.

169. In failing to protect Plaintiffs' and Class Members' Private Information, and in intentionally misusing and/or disclosing their Private Information, Defendant acted with intentional malice and oppression and in conscious disregard of Plaintiffs' and Class Members' rights to have such information kept confidential and private.

170. Plaintiffs seek an award of damages on behalf of themselves and the Class.

THIRD COUNT

NEGLIGENCE *PER SE*

(On Behalf of Plaintiffs and the Class)

171. Plaintiffs repeat and re-allege each and every allegation contained in Paragraphs 1 through 170 as if fully set forth herein.

172. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendant's, of failing to use reasonable measures to protect Private Information. The FTC publications and orders described above also form part of the basis of Defendant's duty in this regard.

173. Defendant violated Section 5 of the FTC Act by failing to use reasonable measures to protect Private Information and not complying with applicable industry standards. Defendant's conduct was particularly unreasonable given the nature and amount of Private Information it obtained and stored, and the foreseeable consequences of the Data Breach for companies of

Defendant's magnitude, including, specifically, the immense damages that would result to Plaintiffs and Members of the Class due to the valuable nature of the Private Information at issue in this case—including Social Security numbers.

174. Defendant's violations of Section 5 of the FTC Act constitute negligence *per se*.

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

176. The harm that occurred as a result of the Data Breach is the type of harm the FTC Act was intended to guard against. The FTC has pursued enforcement actions against businesses, which, as a result of its failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiffs and members of the Class.

177. As a direct and proximate result of Defendant's negligence per se, Plaintiffs and members Class have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity how their PII is used; (iii) the compromise, publication, and/or theft of their PII; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from tax fraud and identity theft; (vi) costs associated with placing freezes on credit reports; (vii) the continued risk to their PII, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII of its current and former employees and customers in its continued possession; and (viii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the

impact of the PII compromised as a result of the Data Breach for the remainder of the lives of Plaintiffs and members of the Class.

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

FOURTH COUNT

BREACH OF IMPLIED CONTRACT

(On Behalf of Plaintiffs and the Customer Sub-class)

179. Plaintiffs repeat and re-allege each and every allegation contained in Paragraphs 1 through 178 as if fully set forth herein.

180. When Plaintiffs and Class Members provided their Private Information to RMCHCS in exchange for Defendant's services, they entered into implied contracts with Defendant pursuant to which Defendant agreed to reasonably protect such information.

181. Defendant solicited and invited Class Members to provide their Private Information as part of Defendant's regular business practices.

182. Plaintiffs and Class Members accepted Defendant's offers and provided their Private Information to Defendant.

183. In entering into such implied contracts, Plaintiffs and Class Members reasonably believed and expected that Defendant's data security practices complied with relevant laws and regulations, including HIPAA, and were consistent with industry standards.

184. Class Members who paid money to Defendant reasonably believed and expected

that Defendant would use part of those funds to obtain adequate data security. Defendant failed to do so.

185. Plaintiffs and Class Members would not have entrusted their Private Information to Defendant in the absence of the implied contract between them and Defendant to keep their information reasonably secure. Plaintiffs and Class Members would not have entrusted their Private Information to Defendant in the absence of its implied promise to monitor its computer systems and networks to ensure that it adopted reasonable data security measures.

186. Plaintiffs and Class Members fully and adequately performed their obligations under the implied contracts with Defendant.

187. Defendant breached its implied contracts with Class Members by failing to safeguard and protect their Private Information.

188. As a direct and proximate result of Defendant's breaches of the implied contracts, Class Members sustained damages as alleged herein.

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

190. Plaintiffs and Class Members are also entitled to injunctive relief requiring Defendant to, *e.g.*, (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) immediately provide adequate credit monitoring to all Class Members.

FIFTH COUNT

BREACH OF FIDUCIARY DUTY

(On Behalf of Plaintiffs and the Customer Sub-classes)

191. Plaintiffs repeat and re-allege each and every allegation contained in Paragraphs 1

through 190 as if fully set forth herein.

192. In light of the special relationship between Defendant and Plaintiffs and Class Members, whereby Defendant became guardians of Plaintiffs' and Class Members' Private Information, Defendant became a fiduciary by its undertaking and guardianship of the Private Information, to act primarily for the benefit of its customers, including Plaintiff and Class Members, (1) for the safeguarding of Plaintiffs' and Class Members' Private Information; (2) to timely notify Plaintiff and Class Members of a data breach and disclosure and (3) maintain complete and accurate records of what customer information (and where) Defendant did and does store.

193. Defendant had a fiduciary duty to act for the benefit of Plaintiffs and Class Members upon matters within the scope of this relationship, in particular, to keep secure the Private Information of its customers.

194. Defendant breached its fiduciary duties to Plaintiffs and Class Members by failing to diligently discover, investigate and give notice of the Data Breach in a reasonable and practicable period of time.

195. Defendant breached its fiduciary duties to Plaintiffs and Class Members by failing to encrypt and otherwise protect the integrity of the systems containing Plaintiffs' and Class Members' Private Information.

196. Defendant breached its fiduciary duties owed to Plaintiffs and Class Members by failing to timely notify and/or warn Plaintiffs and Class Members of the Data Breach.

197. Defendant breached its fiduciary duties owed to Plaintiffs and Class Members by failing to ensure the confidentiality and integrity of electronic PHI Defendant created, received, maintained, and transmitted, in violation of 45 C.F.R. § 164.306(a)(1).

198. Defendant breached its fiduciary duties owed to Plaintiffs and Class Members by failing to implement technical policies and procedures for electronic information systems that maintain electronic PHI 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).

199. Defendant breached its fiduciary duties owed to Plaintiffs and Class Members by failing to implement policies and procedures to prevent, detect, contain, and correct security violations, in violation of 45 C.F.R. § 164.308(a)(1).

200. Defendant breached its fiduciary duties owed to Plaintiffs and Class Members by failing to identify and respond to suspected or known security incidents and to mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity in violation of 45 C.F.R. § 164.308(a)(6)(ii).

201. Defendant breached its fiduciary duties owed to Plaintiffs and Class Members by failing to protect against any reasonably-anticipated threats or hazards to the security or integrity of electronic PHI in violation of 45 C.F.R. § 164.306(a)(2).

202. Defendant breached its fiduciary duties owed to Plaintiffs and Class Members by failing to protect against any reasonably anticipated uses or disclosures of electronic PHI that are not permitted under the privacy rules regarding individually identifiable health information in violation of 45 C.F.R. § 164.306(a)(3).

203. Defendant breached its fiduciary duties owed to Plaintiffs and Class Members by failing to ensure compliance with the HIPAA security standard rules by its workforce in violation of 45 C.F.R. § 164.306(a)(94).

204. Defendant breached its fiduciary duties owed to Plaintiffs and Class Members by impermissibly and improperly using and disclosing PHI that is and remains accessible to

unauthorized persons in violation of 45 C.F.R. § 164.502, et seq.

205. Defendant breached its fiduciary duties owed to Plaintiffs and Class Members by failing to effectively train all Members of its workforce (including independent contractors) on the policies and procedures with respect to PHI as necessary and appropriate for the Members of its workforce to carry out their functions and to maintain security of PHI in violation of 45 C.F.R. § 164.530(b) and 45 C.F.R. § 164.308(a)(5).

206. Defendant breached its fiduciary duties owed to Plaintiffs and Class Members by failing to design, implement, and enforce policies and procedures establishing physical and administrative safeguards to reasonably safeguard PHI, in compliance with 45 C.F.R. § 164.530(c).

207. Defendant breached its fiduciary duties to Plaintiffs and Class Members by otherwise failing to safeguard Plaintiffs' and Class Members' Private Information.

208. As a direct and proximate result of Defendant's breach of its fiduciary duties, Plaintiffs and Class Members have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the compromise, publication, and/or theft of their Private Information; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft and/or unauthorized use of their Private Information; (iv) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (v) the continued risk to their Private Information, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information in its continued possession; (vi) future costs in terms

of time, effort, and money that will be expended as result of the Data Breach for the remainder of the lives of Plaintiffs and Class Members and (vii) the diminished value of Defendant's services they received.

209. As a direct and proximate result of Defendant's breaching its fiduciary duties, Plaintiffs and Class Members have suffered and will continue to suffer other forms of injury and/or harm, and other economic and non-economic losses.

SIXTH COUNT

UNJUST ENRICHMENT

(On Behalf of Plaintiffs and the Customer Sub-Classes)

210. Plaintiffs repeat and re-allege each and every allegation contained in Paragraphs 1 through 209 as if fully set forth herein.

211. This count is plead in the alternative to Counts 3 and 4 (breach of express and breach of implied contract).

212. Plaintiffs and Class Members conferred a monetary benefit on Defendant, by paying Defendant money for healthcare services, a portion of which was to have been used for data security measures to secure Plaintiffs' and Class Members' PII and PHI, and by providing Defendant with their valuable PII and PHI.

213. Defendant enriched itself by saving the costs it reasonably should have expended on data security measures to secure Plaintiffs' and Class Members' PII and PHI.

214. Instead of providing a reasonable level of security that would have prevented the Data Breach, Defendant instead calculated to avoid their data security obligations at the expense of Plaintiffs and Class Members by utilizing cheaper, ineffective security measures. Plaintiffs and Class Members, on the other hand, suffered as a direct and proximate result of Defendant's failure

to provide the requisite security.

215. Under the principles of equity and good conscience, Defendant should not be permitted to retain the money belonging to Plaintiffs and Class Members, because Defendant failed to implement appropriate data management and security measures that are mandated by industry standards.

216. Defendant acquired the monetary benefit and PII and PHI through inequitable means in that it failed to disclose the inadequate security practices previously alleged.

217. If Plaintiffs and Class Members knew that Defendant had not secured their PII and PHI, they would not have agreed to provide their PII and PHI to Defendant.

218. Plaintiffs and Class Members have no adequate remedy at law.

219. As a direct and proximate result of Defendant's conduct, Plaintiffs and Class Members have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity how their PII is used; (iii) the compromise, publication, and/or theft of their PII and PHI; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, and/or unauthorized use of their PII and PHI; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (vi) the continued risk to their PII and PHI, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fail to undertake appropriate and adequate measures to protect PII and PHI in their continued possession and (vii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PII and PHI compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and

Class Members.

220. As a direct and proximate result of Defendant's conduct, Plaintiffs and Class Members have suffered and will continue to suffer other forms of injury and/or harm.

221. Defendant should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiffs and Class Members, proceeds that they unjustly received from them. In the alternative, Defendant should be compelled to refund the amounts that Plaintiffs and Class Members overpaid for Defendant's services.

SEVENTH COUNT

NEW MEXICO UNFAIR PRACTICES ACT, NMSA 1978, §§ 57-12-2, *et seq.*

(On Behalf of Plaintiffs Charlie and Lacy & the New Mexico Customer Sub-class)

222. Plaintiffs repeat and re-allege each and every allegation contained in Paragraphs 1 through 221 as if fully set forth herein.

223. This claim is brought under the laws of New Mexico and on behalf of all other natural persons whose Private Information was compromised as a result of the Data Breach and reside in states having similar laws regarding unfair practices.

224. RMCHCS is a "person" as meant by NMSA 1978, § 57-12-2.

225. RMCHCS was engaged in "trade" and "commerce" as meant by NMSA 1978, § 57-12-2(C) when engaging in the conduct alleged.

226. The New Mexico Unfair Practices Act, NMSA 1978, §§ 57-12-2, *et seq.*, prohibits both unfair or deceptive trade practices and unconscionable trade practices in the conduct of any trade or commerce.

227. RMCHCS engaged in unconscionable, unfair, and deceptive acts and practices in connection with the sale of goods or services in the regular course of its trade or commerce,

including the following:

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

b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and the Customer Subclass, including duties imposed by the FTC Act, 15 U.S.C. § 45, the GLBA, 15 U.S.C. § 6801, *et seq.*, HIPAA, 42 U.S.C. § 1320d, COPPA, 15 U.S.C. §§ 6501-6505, and New Mexico statutes requiring protections for social security numbers, N.M. Stat. § 57-12B-3(D), and mandating reasonable data security, N.M. Stat. § 57-12C-4, which was a direct and proximate cause of the Data Breach;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff and the Customer Subclass members' Private Information, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs and the Customer Subclass members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, the GLBA, 15 U.S.C. § 6801, *et seq.*, HIPAA, 42 U.S.C. § 1320d, COPPA, 15 U.S.C. §§ 6501-6505, and New Mexico statutes requiring protections for social security numbers, N.M. Stat. § 57-12B-3(D), and mandating reasonable data security, N.M. Stat. § 57-12C-4;

f. Failing to timely and adequately notify Plaintiffs and the Customer Subclass members of the Data Breach;

g. Misrepresenting that certain sensitive Personal Information was not accessed during the Data Breach, when it was;

h. Omitting, suppressing and concealing the material fact that it did not reasonably or adequately secure Plaintiffs and the Customer Subclass members' Private Information and

i. Omitting, suppressing and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs and the Customer Subclass members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, the GLBA, 15 U.S.C. § 6801, *et seq.*, HIPAA, 42 U.S.C. § 1320d, COPPA, 15 U.S.C. §§ 6501-6505, and New Mexico statutes requiring protections for

social security numbers, NMSA 1978, § 57-12B-3(D), and mandating reasonable data security, NMSA 1978, § 57-12C-4.

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

229. RMCHCS's representations and omissions were material because they were likely to deceive reasonable consumers, including Plaintiffs and the Customer Subclass members, that their Private Information was not exposed and misled Plaintiffs and the New Mexico Subclass members into believing they did not need to take actions to secure their identities.

230. RMCHCS intended to mislead Plaintiff and New Mexico Subclass members and induce them to rely on its misrepresentations and omissions.

231. RMCHCS acted intentionally, knowingly and maliciously to violate New Mexico's Unfair Practices Act, and recklessly disregarded Plaintiff and the Customer Subclass members' rights.

232. As a direct and proximate result of RMCHCS's unfair, deceptive, and unconscionable trade practices, Plaintiff and the Customer Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft and loss of value of their Private Information.

233. Plaintiff and the Customer Subclass members seek all monetary and non-monetary relief allowed by law, including injunctive relief, actual damages or statutory damages of $100 (whichever is greater), treble damages or statutory damages of $300 (whichever is greater), and reasonable attorneys' fees and costs.

EIGHTH COUNT

ARIZONA CONSUMER FRAUD ACT, Ariz. Rev. Stat. §§ 44-1521, *et seq.*

(On Behalf of Plaintiffs E.H. and Tsosie & the Arizona Customer Sub-class)

234. Plaintiffs repeat and re-allege each and every allegation contained in Paragraphs 1 through 233 as if fully set forth herein.

235. This claim is brought individually under the laws of Arizona and on behalf of all other natural persons whose Private Information was compromised as a result of the Data Breach and reside in states having similar laws regarding consumer fraud.

236. RMCHCS is a "person" as defined by Ariz. Rev. Stat. § 44-1521(6).

237. RMCHCS advertised, offered or sold goods or services in Arizona and engaged in trade or commerce directly or indirectly affecting the people of Arizona.

238. RMCHCS engaged in deceptive and unfair acts and practices, misrepresentation, and the concealment, suppression and omission of material facts affecting the people of Arizona in connection with the sale and advertisement of "merchandise" (as defined in Arizona Consumer Fraud Act, Ariz. Rev. Stat. § 44-1521(5)) in violation of Ariz. Rev. Stat. § 44-1522(A), including:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and Arizona Subclass members' Private Information, which was a direct and proximate cause of the Data Breach;

b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Arizona Subclass members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, the GLBA, 15 U.S.C. § 6801, *et seq.*, HIPAA, 42 U.S.C. § 1320d, and COPPA, 15 U.S.C. §§ 6501-05, which was a direct and proximate cause of the Data Breach;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff and Arizona Subclass members' Private Information, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Arizona Subclass members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, the GLBA, 15 U.S.C. § 6801, *et seq.*, HIPAA, 42 U.S.C. § 1320d, and COPPA, 15 U.S.C. §§ 6501-05;

f. Failing to timely and adequately notify the Social Good Entities, Plaintiffs, and Arizona Subclass members of the Data Breach;

g. Misrepresenting that certain sensitive Personal Information was not accessed during the Data Breach, when it was;

h. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff and Arizona Subclass members' Private Information and

i. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Arizona Subclass members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, the GLBA, 15 U.S.C. § 6801, *et seq.*, HIPAA, 42 U.S.C. § 1320d, and COPPA, 15 U.S.C. §§ 6501-05.

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

240. RMCHCS's representations and omissions were material because they were likely to deceive reasonable consumers, including Plaintiffs and the Arizona Subclass members, that their Private Information was not exposed and misled Plaintiffs and the Arizona Subclass members into believing they did not need to take actions to secure their identities.

241. RMCHCS intended to mislead Plaintiff and Arizona Subclass members and induce them to rely on its misrepresentations and omissions.

242. Had RMCHCS disclosed to Plaintiffs and Class members that its data systems were

not secure and, thus, vulnerable to attack, RMCHCS would have been unable to continue in business and it would have been forced to adopt reasonable data security measures and comply with the law. Instead, RMCHCS was trusted with sensitive and valuable Private Information regarding millions of consumers, including Plaintiffs, the Class, and the Arizona Subclass. RMCHCS accepted the responsibility of being a steward of this data while keeping the inadequate state of its security controls secret from the public. Accordingly, because RMCHCS held itself out as maintaining a secure platform for Private Information data, Plaintiffs, the Class, and the Arizona Subclass members acted reasonably in relying on RMCHCS's misrepresentations and omissions, the truth of which they could not have discovered.

243. RMCHCS acted intentionally, knowingly, and maliciously to violate Arizona's Consumer Fraud Act, and recklessly disregarded Plaintiff and Arizona Subclass members' rights.

244. As a direct and proximate result of RMCHCS's unfair and deceptive acts and practices, Plaintiff and Arizona Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their Private Information.

245. Plaintiff and Arizona Subclass members seek all monetary and non-monetary relief allowed by law, including compensatory damages; disgorgement; punitive damages; injunctive relief; and reasonable attorneys' fees and costs.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs Alicia Charlie, Leona Garcia Lacy, Darrell Tsosie and E.H., a minor, by and through his guardian Gary Hicks, individually and on behalf of all others similarly situated, pray for judgment against Rehoboth McKinley Christian Health Care Services as follows:

a) For an Order certifying this action as a class action and appointing Plaintiffs and their counsel to represent the classes;

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

c) For equitable relief compelling Defendant to utilize appropriate methods and policies with respect to consumer data collection, storage and safety, and to disclose with specificity the type of PII and PHI compromised during the Data Breach;

d) For equitable relief requiring restitution and disgorgement of the revenues wrongfully retained as a result of Defendant's wrongful conduct;

e) Ordering Defendant to pay for not less than three years of credit monitoring services for Plaintiffs and the Class;

f) For an award of actual damages, compensatory damages, statutory damages, and statutory penalties, in an amount to be determined, as allowable by law;

g) For an award of punitive damages, as allowable by law;

h) For an award of attorneys' fees and costs, and any other expense, including expert witness fees;

i) Pre- and post-judgment interest on any amounts awarded and

j) Such other and further relief as this court may deem just and proper.

JURY TRIAL DEMANDED

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

Dated: June 4, 2021

Respectfully Submitted,

By: /s/ Kristina Martinez

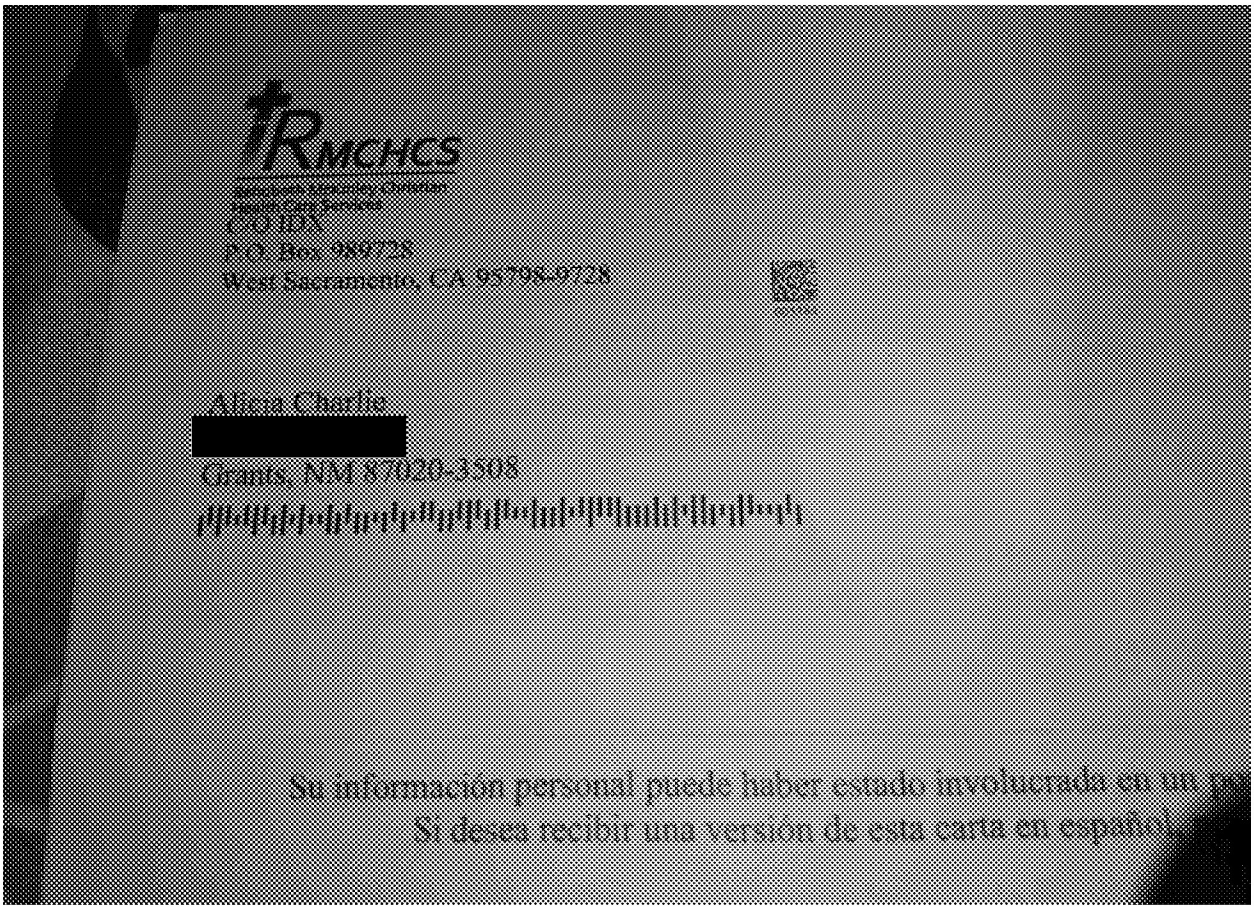
Kristina Martinez
EGOLF + FERLIC +
MARTINEZ + HARWOOD, LLC
123 W. San Francisco St., Second Floor
Santa Fe, NM 87501
(505) 986-9641
kmartinez@EgolfLaw.com

MASON LIETZ & KLINGER LLP
Gary E. Mason (*pro hac vice forthcoming*)
David K. Lietz (*pro hac vice forthcoming*)
5101 Wisconsin Ave., NW, Ste. 305
Washington, DC 20016
Phone: 202.640.1160
gmason@masonllp.com
dlietz@masonllp.com

Gary M. Klinger (*pro hac vice forthcoming*)
MASON LIETZ & KLINGER LLP
227 W. Monroe Street, Suite 2100
Chicago, IL 60606
Tel.: (202) 975-0477
gklinger@masonllp.com

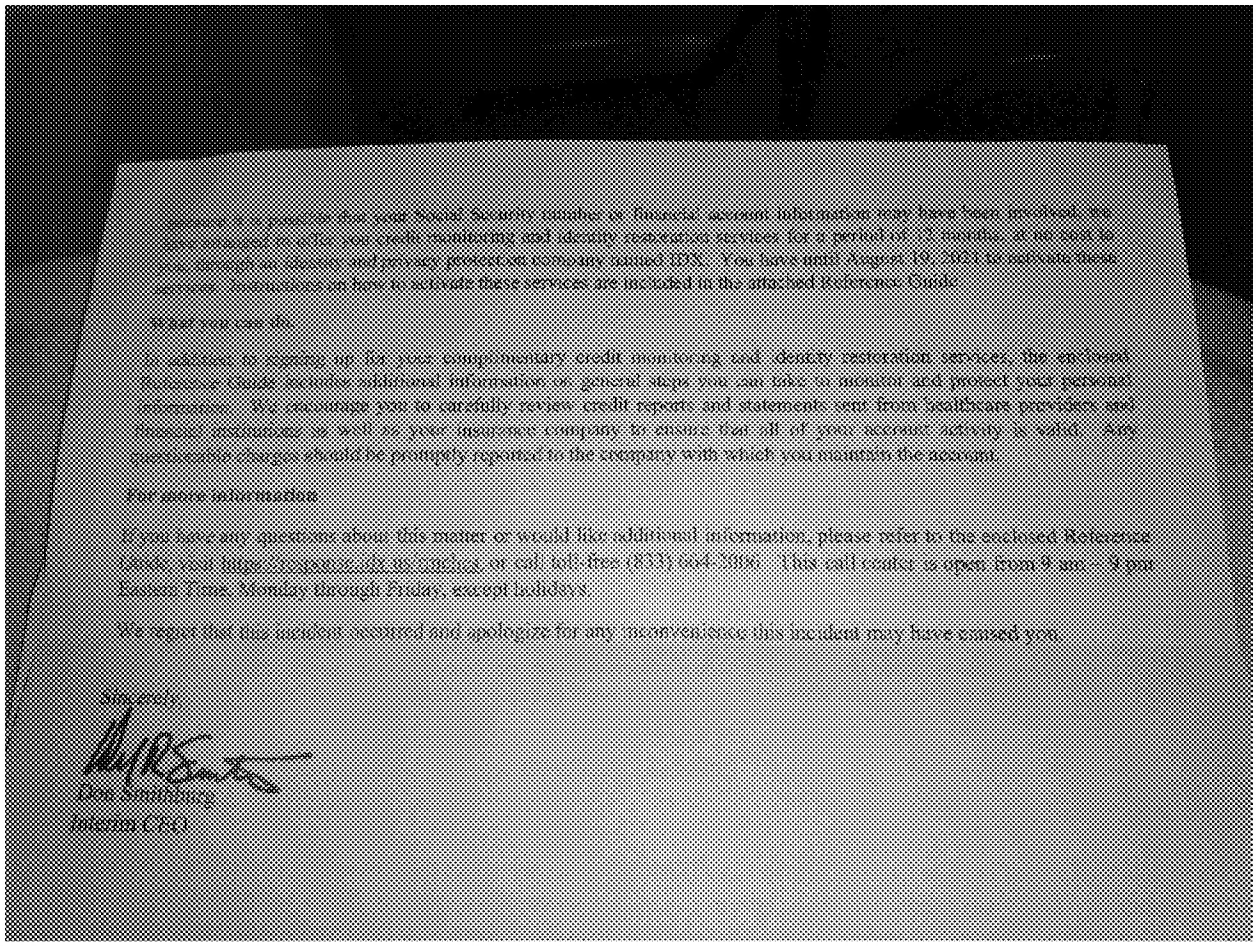
Attorneys for Plaintiffs & the Proposed Class

Exhibit A


RMCHCS
Rocky Mountain Consortium for Health Care Services
CCOHA
P.O. Box 989728
West Sacramento, CA 95798-9728
Alicia Charlie
Grants, NM 87020-3508
Su información personal puede haber estado involucrada en un
Si desea recibir una versión de esta carta en español

What we are doing

Since 2015, the security of personal information very seriously. As soon as we discovered the incident, we immediately launched a security investigation, contacted law enforcement, and took steps to remediate the incident. In addition, to help prevent this type of incident from occurring again, we have enhanced our security and monitoring as well as hardened our systems as appropriate to minimize the risk of any similar incident in the future.



Jane Doe
Interim CEO

Exhibit B

RMCHCS
Rehoboth McKinley Christian
Health Care Services
C/O IDX
P.O. Box 989728
West Sacramento, CA 95798-9728

Elijah Hicks
[redacted]
Saint Johns, AZ [redacted]

[redacted]

Su información personal puede haber estado involucrada en un posible incidente de seguridad
Si desea recibir una versión de esta carta en español, por favor llame al 833-664-3018

Notice of Data Breach

To Elijah Hicks:

Rehoboth McKinley Christian Health Care Services (RMCHCS) deeply values the trust and service [illegible] their families. That is why we are writing to inform you about a data security incident that may have involved some of your personal information. [illegible] you should also be provided [illegible] of any [illegible] activity.

How to Enroll in IDX Credit Monitoring Protection Services

As a safeguard, we have arranged for you to enroll, at no cost to you, in an online credit [illegible] protection service provided by IDX.

To enroll in this service, please call 833-664-3018 or visit https://app.idx.us/account-creation/protect and [illegible] Enrollment Code: [illegible]. This service includes [illegible] monitoring included in the membership must be activated to be effective. Please note [illegible] access to a computer and the internet to use this service. If you need assistance, IDX will [illegible] encourage you to take advantage of these protections and remain vigilant for incidents [illegible] by regularly reviewing and monitoring your credit reports and account statements.

Contact the U.S. Federal Trade Commission

If any unauthorized transactions on any of your financial accounts. Promptly [illegible] or financial institution. If you detect any incidents of identity theft or fraud, [illegible] & enforcement authorities, state Attorney General and the FTC.

Exhibit C

C/O IDX
P.O. Box 989728
West Sacramento, CA 95798-9728

Leonor Cuevas
PO Box [redacted]
Commerce, CA 90012-0163

[illegible]

Su información personal puede haber estado involucrada en un posible incidente
Si desea recibir una versión de esta carta en español, por favor llame al [illegible]

Notice of Data Breach

Dear Leonor Cuevas:

Rancho Los Amigos National Rehabilitation Center (RMC|HCS) deeply values the trust [illegible] their families. That is why we are writing to inform you of a data security incident that [illegible] information. We are committed to transparency and want to share more about what happ[illegible] address this issue and minimize the risk of any similar incident in the future.

What happened?

On February 16, 2023, we learned that certain patient information may have been [illegible] as a result of potential unauthorized activity that we had been investigating. We promptly [illegible] firm to further investigate the incident and assist with remediation efforts. On [illegible] unauthorized party was able to access certain systems that contained patient information [illegible] January 24 and February 8, 2023. As a result of our review, on April 30, 2023, we [illegible] personal information may have been involved.

What information may have been involved?

The patient information may have included: (1) information to identify and contact [illegible] birth, address, telephone number, and email address; (2) Social Security number; a

Exhibit D

RMCHCS

C/O IDX
P.O. Box 989728
West Sacramento, CA 95798-9728

Darrell Tsosie
PO Box
Fort Defiance, AZ 86504

[illegible]

Su información personal puede haber estado involucrada en un posible incidente de seguridad de datos.
Si desea recibir una versión de esta carta en español, por favor llame [illegible]

Notice of Data Breach

To Darrell Tsosie:

Rehoboth McKinley Christian Health Care Services (RMCHCS) deeply values the trust and support of our patients and their families. That is why we are writing to inform you of a data security incident that may have affected your [illegible] information. We are committed to transparency and want to share more about what happened and the measures taken to address this issue and minimize the risk of any similar incident in the future.

What happened?

On February 16, 2021, we learned that certain patient information may have been removed from [illegible] as a result of potential unauthorized activity that we had been investigating. We promptly engaged a third-party [illegible] firm to further investigate the incident and assist with remediation efforts. Our investigation has found that an unauthorized party was able to access certain systems that contained patient information and remove some data between January 21 and February 5, 2021. As a result of our review, on April 30, 2021, we [illegible] personal information may have been involved.

What information may have been involved?

The patient information may have included: (1) information to identify and contact [illegible] birth, address, telephone number and email address, (2) Social Security number, [illegible] number, and/or tribal ID number, (3) health insurance information, such as name of [illegible] number, (4) medical information, such as Medical Record Number, dates of service, [illegible] information, treatment, and diagnosis information, and (5) billing and claims [illegible] information. Please note that not all data elements may have been involved for all individuals.

What we are doing.

RMCHCS takes the security of personal information very seriously. As soon as we [illegible] promptly launched a forensic investigation, contacted law enforcement, and took steps to [illegible] response to this incident, we have enhanced our security and monitoring as well as [illegible] to minimize the risk of any similar incident in the future.