STATE OF NEW MEXICO
COUNTY OF BERNALILLO
SECOND JUDICIAL DISTRICT

JESSE MARTINEZ and KYRA NIETO, individually and on behalf of all others similarly situated, Plaintiffs, v. PRESBYTERIAN HEALTHCARE SERVICES, Defendant.	)	Case No. D-202-CV-2020-01578 Consolidated with Case Nos. 1:20-cv-00191-SMV-JFR, D-202-CV-2020-02651 JURY TRIAL DEMANDED
MICHAEL O. GARCIA, individually and on behalf of all others similarly situated, Plaintiff, v. PRESBYTERIAN HEALTHCARE SERVICES, Defendant.	)	
JUAN GONZALES, individually an on behalf of all others similarly situated, Plaintiff, v. PRESBYTERIAN HEALTHCARE SERVICES, Defendant.	)	

CONSOLIDATED CLASS ACTION COMPLAINT

Plaintiffs, Jesse Martinez, Kyra Nieto, Michael O. Garcia, and Juan Gonzales, individually and on behalf of all others similarly situated, bring this action against Defendant Presbyterian Healthcare Services ("Presbyterian"), and allege as follows:

NATURE OF THE ACTION

1. On or about November 25, 2019, Presbyterian notified Plaintiffs and its other current and former patients that it had "discovered anonymous, unauthorized access gained through a deceptive email to some of Presbyterian's workforce members" and that it "believe[s] that the unauthorized access to these email accounts was part of a scam or deceptive email trying to get information, known as 'phishing.'"

2. According to the November 25 letter (the "notification letter"), attached hereto as Exhibit A, and the Data Disclosure notification page on Presbyterian's website, attached hereto as Exhibit B, Plaintiffs and other patients' personal health information ("PHI")—including, patients' names, dates of birth, Social Security numbers, and clinical and/or health information—was compromised in the phishing attack (the "Data Disclosure").

3. The notification letter explained that Presbyterian's investigation determined an unauthorized third party had received unauthorized access to "certain affected email accounts" that contained patients' PHI. Ex. A.

4. The notification letter urged Plaintiffs and other Presbyterian patients to "review the statements that you receive from your health plan or your health care providers regarding your health care services" and to "contact the health plan or provider immediately" if they "see any service that you believe you did not receive." *Id.*

5. As a consequence of the Data Disclosure, Plaintiffs' and Class members' sensitive PHI has been released into the public domain and they have had to, and will continue to have to, spend time to protect themselves from fraud and identity theft.

6. Further, and to compound the harm, Presbyterian knew about the Data Disclosure for nearly six months before Presbyterian notified Plaintiffs and its other patients. The notification letter states that Presbyterian knew about the Data Disclosure by June 6, 2019; however, Presbyterian did not notify Plaintiffs and other patients that their sensitive PHI had been compromised until at least November 25, 2019.

7. As a result of the Data Disclosure, Plaintiffs and Class members have been required to take measures to deter and detect identity theft and fraud. Plaintiffs and Class members have been required to take the time and effort, which they otherwise would have dedicated to other life demands, to mitigate the actual and likely impact of the Data Disclosure including, *inter alia*, closely reviewing and monitoring their credit reports, financial accounts, explanations of benefits, and medical accounts for unauthorized activity, placing "freezes" and "alerts" with credit reporting agencies, contacting their medical and financial institutions, and closing or modifying financial accounts.

8. Plaintiffs bring this class action against Presbyterian for failing to adequately secure and safeguard the PHI of Plaintiffs and the Class, breaching the terms of Presbyterian's implied contracts with its patients, failing to comply with industry standards regarding the use and transmission of PHI, and providing inaccurate and inadequate notice to Plaintiffs and other Class members as to precisely how their sensitive PHI had been accessed by unauthorized persons.

9. Plaintiffs' and the Class members' information was maintained on Presbyterian's computer network. Upon information and belief, the mechanism of the Data Disclosure and

potential for improper disclosure of Plaintiffs' and Class members' Private Information was a known risk to Presbyterian, and thus Presbyterian was on notice that failing to take steps necessary to secure the PHI from those risks left that property in a dangerous condition.

10. In addition, Presbyterian and its employees failed to properly monitor the computer network and systems that housed the PHI. Had Presbyterian properly monitored its property, it would have discovered the intrusion sooner.

11. Presbyterian disregarded the rights of Plaintiffs and Class members by intentionally, willfully, recklessly, or negligently failing to take and implement adequate and reasonable measures to ensure that the PHI it stores was safeguarded; failing to take available steps to prevent the Data Disclosure from happening; and failing to follow the mandatory, applicable, and appropriate protocols, policies, and procedures.

12. Plaintiffs' and Class members' identities are now at risk because of Presbyterian's negligent conduct since the PHI that Presbyterian collected and maintained is now in the hands of data thieves.

13. Armed with the PHI accessed in the Data Disclosure, data thieves can commit a variety of crimes 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 giving false information to police during an arrest.

14. As the direct result of Presbyterian's actions, the PHI of Plaintiffs and Class members was compromised and disclosed to unauthorized third parties. Plaintiffs and Class members have been exposed to a heightened and imminent risk of fraud and identity theft. Plaintiffs and Class members must now and in the future closely monitor their financial accounts to guard against identity theft. Plaintiffs and Class members may also incur out of pocket costs for, *inter alia*, purchasing credit monitoring services, credit freezes, credit reports, or other protective measures required to deter and detect identity theft.

15. Further, because Plaintiffs' and Class members' information remains stored in Presbyterian's systems, Plaintiffs and Class members have an interest in ensuring that Presbyterian takes the appropriate measures to protect their information against future unauthorized disclosures.

PARTIES

16. Plaintiff Jesse Martinez is a citizen and resident of New Mexico.

17. Plaintiff Kyra Nieto is a citizen and resident of New Mexico.

18. Plaintiff Michael Garcia is a citizen and resident of New Mexico.

19. Plaintiff Juan Gonzales is a citizen and resident of New Mexico.

20. Plaintiffs are current and former patients at Presbyterian and their PHI was stored on Presbyterian's system at all times material hereto.

21. Plaintiffs are among the 183,370 patients whose PHI was disclosed during the Data Disclosure and Plaintiffs received the notification letter from Presbyterian informing them for the first time that their PHI had been compromised. Plaintiff Nieto also received notification letters for her husband and their five minor children.

22. Defendant Presbyterian Healthcare Services is a New Mexico corporation with its headquarters in Albuquerque, New Mexico.

JURISDICTION AND VENUE

23. This Court has general personal jurisdiction over Presbyterian because Presbyterian is at home in this State.

24. Venue is likewise proper in this County pursuant to N.M. Stat. § 38-3-1(A) because Bernalillo County is the county in which Presbyterian maintains its principal office.

FACTUAL ALLEGATIONS

A. Presbyterian's Business

25. Presbyterian is a private not-for-profit health care system and health care provider and is in the business of rendering healthcare services, medical care, and treatment.

26. Presbyterian owns and operates 8 hospitals throughout New Mexico. Presbyterian also operates Presbyterian Health Plan.

27. Presbyterian provides medical care and treatment in the following broad areas: Primary Care; Urgent Care; Women's Care; Children's Health; Cancer Care; Heart and Vascular Care; Neuroscience; Behavioral Health; Surgery; Specialties (consisting of 13 specialty care areas of practice); a Bariatric Center; Infusion Services; Transplant Services; Sleep Medicine; a Wound and Ostomy Center; Emergency Care; Healthcare at Home; Hospice, Palliative Care, and; Supporting Services (consisting of 8 service categories).[1]

28. Presbyterian requires that all patients entrust it with certain personal and medical information as a condition of treatment, including name, address, phone number, email address, date of birth, demographic information, Social Security number, information relating to individual medical history, insurance information and coverage, information concerning an individual's

[1] *Specialty Clinics & Medical Centers*, PRESBYTERIAN HEALTHCARE, https://www.Presbyterian.org/doctors-services/services-centers/Pages/default.aspx (last visited July 24, 2020).

doctor, nurse or other medical providers, photo identification, employer information, and other information that may be deemed necessary to provide care.

29. Presbyterian also gathers medical information about patients and creates records of the care it provides to them.

30. All of Presbyterian's employees, staff, entities, clinics, sites, and locations may share patient information with each other for various purposes without a written authorization, as disclosed in the Joint Notice of Privacy Practices (the "Privacy Notice"), attached hereto as Exhibit C. Presbyterian maintains this personal and medical information in its ordinary course of business.

31. The Privacy Notice is provided to every patient upon request and is posted on Presbyterian's website. The Privacy Notice notes that Presbyterian is required to ask every patient "for a written acknowledgement that you have received a copy" of the Privacy Notice. Ex. C at 1.

32. Because of the highly sensitive and personal nature of the information Presbyterian acquires and stores with respect to its patients, Presbyterian promises, among other things, to (1) "maintain the privacy of your health information"; (2) inform and notify patients "when your protected health information has been inappropriately accessed, used, or disclosed as a result of a breach"; and (3) not "use or share your health information without your written authorization unless required by law or as described in this Joint Notice of Privacy Practices." *Id.* at 1, 3.

33. Presbyterian also publishes a written statement under the heading "Patient Rights" on its website (the "Patient Rights document") that promises Presbyterian patients have the right "[t]o have confidentiality of your medical records and personal information as further described in the Joint Notice of Privacy Practices handout."[2]

[2] *You Have the Right*, PRESBYTERIAN HEALTHCARE 2 (Sept. 2018), http://docs.Presbyterian.org/idc/groups/public/%40Presbyterian/%40marketing/documents/Presbyteriancontent/pel_00182934.pdf

34. As current and former patients at Presbyterian, Plaintiffs and Class members provided their PHI to Presbyterian for purposes of treatment. Plaintiffs and Class members relied on Presbyterian to keep their highly sensitive information confidential and securely maintained and would not have provided this information if not for Presbyterian's promises to maintain it securely.

B. The Data Disclosure

35. On or about November 25, 2019, Presbyterian advised Plaintiffs and the Class that "some" Presbyterian employees' accounts had been compromised as part of a "scam or deceptive email trying to get information, known as 'phishing.'" Ex. A. The unauthorized third party had access to certain employees' accounts from May 9, 2019 until at least June 6, 2019, when Presbyterian discovered the breach and began securing the affected email accounts.

36. According to the notification letter and other materials published by Presbyterian, the phishing attack had compromised a wide range of confidential information, including the patient's name, date of birth, Social Security number, and clinical and/or health information. *See* Exs. A and B.

37. Despite the fact that Presbyterian promises consumers in its Privacy Notice that it has mechanisms in place to discover when its computer systems are breached, it nevertheless concedes it was unaware of the cyberattack for nearly a month, from May 9, 2019 until June 6, 2019.

38. The breach that compromised Plaintiffs' and Class members' information originated from the Presbyterian email system and resulted from multiple employees being fooled by a phishing scam. Employees responding to the phishing email inadvertently disclosed their

login credentials to the attacker who then used the credentials to remotely access their email accounts.

39. The compromised email accounts contained messages and email attachments that included PHI of at least 183,000 patients.

40. Upon information and belief, Plaintiffs believe their PHI was stolen in the Data Disclosure and subsequently sold.

41. Presbyterian did not bother to notify affected patients until August 2, 2019, nearly two months after the Data Disclosure was discovered, and nearly 3 months after the Data Disclosure initially occurred.

42. Even worse, on July 31, 2019, Presbyterian learned that a yet another unauthorized person accessed employee email accounts through phishing, and that at least one of the email accounts accessed contained provider names and Social Security numbers.

43. As a result, Presbyterian sent supplemental notice to the providers affected, including Presbyterian-employed providers, and offered the providers complimentary credit monitoring. To date, Presbyterian has not offered patients affected by the Data Disclosure any complimentary credit monitoring.

44. To the contrary, Plaintiffs and other recipients of the notification letter have been informed that Presbyterian is not offering credit monitoring services to affected individuals.

45. Presbyterian had obligations created by HIPAA, Presbyterian's contract, industry standards, common law, and representations made to Plaintiffs and the Class, to keep the PHI entrusted to it confidential and to protect it from unauthorized access and disclosure.

46. Plaintiffs and Class members provided their PHI to Presbyterian with the reasonable expectation and mutual understanding that Presbyterian would comply with its obligations to keep such information confidential and secure from unauthorized access.

47. Presbyterian could have easily prevented this Data Disclosure. Presbyterian is aware of the value of PHI and the risks associated with unauthorized disclosure of this information, yet it failed to implement adequate measures to protect its patients' information.

48. Presbyterian's data security obligations were particularly important given the substantial increase in cyberattacks and data breaches in the healthcare industry preceding the Data Disclosure.

49. Indeed, cyberattacks have become so notorious that the Federal Bureau of Investigation ("FBI") and U.S. Secret Service have issued a warning to potential targets so they are aware of, and prepared for, a potential attack. As one report explained, "[e]ntities like smaller municipalities and *hospitals* are attractive to ransomware criminals . . . because they often have lesser IT defenses and a high incentive to regain access to their data quickly."[3]

50. Therefore, the increase in such attacks, and attendant risk of future attacks, was widely known to the public and throughout the healthcare industry.

51. Despite this widespread knowledge of the dangers of identity theft and fraud associated with phishing schemes and unauthorized disclosure of PHI, Presbyterian provided unreasonably deficient protections prior to the Data Disclosure, including but not limited to a lack of security measures for storing and handling patients' PHI and inadequate employee training regarding how to access, handle, and safeguard this information.

[3] Ben Kochman, *FBI, Secret Service Warn of Targeted Ransomware*, Law 360 (NOV. 18, 2019), https://www.law360.com/consumerprotection/articles/1220974/fbi-secret-service-warn-of-targeted-ransomware?nl_pk=3ed44a08-fcc2-4b6c-89f0-aa0155a8bb51&utm_source=newsletter&utm_medium=email&utm_campaign=consumerprotection.

52. Presbyterian failed to adequately adopt and train its employees on even the most basic of information security protocols, including:

a. storing, locking, encrypting, and limiting access to patients' highly sensitive PHI;

b. implementing guidelines for accessing, maintaining, and communicating sensitive PHI; and

c. protecting patients' sensitive PHI by implementing protocols on how to utilize such information.

53. Presbyterian further breached its obligations to Plaintiffs and the Class and/or was otherwise negligent and reckless because it failed to properly maintain and safeguard its own computer systems. Presbyterian'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 protect patients' PHI;

c. failing to monitor Presbyterian's data security systems for existing intrusions;

d. failing to ensure that Presbyterian's vendors with access to its computer systems and data employed reasonable security procedures;

e. 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);

f. 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);

g. 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);

h. 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);

i. 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);

j. 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);

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

l. 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); and/or

m. failing to render the electronic PHI it maintained unusable, unreadable, or indecipherable to unauthorized individuals, as Presbyterian 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.

54. Presbyterian's failures handed Plaintiffs' and Class members' PHI over to an unknown and unauthorized third party and put Plaintiffs and the Class at serious, immediate, and continuous risk of identity theft and fraud.

55. PHI that is jeopardized in Data Disclosures like the one at issue here are often sold, purchased, and used to perpetuate identity theft and fraud by unlawful recipients.

56. The Data Disclosure that exposed Plaintiffs' and Class members' PHI was caused by Presbyterian's violation of its obligations to abide by best practices and industry standards concerning its information security practices and processes. Presbyterian failed to comply with security standards or to implement security measures that could have prevented or mitigated the Data Disclosure.

C. Ramifications of the Data Disclosure

57. The ramifications of Presbyterian's failure to keep its patients' PHI secure are long lasting and severe. Once PHI is stolen, fraudulent use of that information and damage to victims may continue for years.

58. The Federal Trade Commission ("FTC") defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority." 17 C.F.R. § 248.201 (2013). The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, an individual's name, Social Security number, and date of birth. *Id.*

59. Social Security numbers and medical records are among the worst types of personal information to have stolen because they may be put to a variety of fraudulent uses and are difficult for an individual to change.

60. The Social Security Administration has warned that identity thieves can use an individual's Social Security number to apply for additional credit lines. Such fraud may go undetected until debt collection calls commence months, or even years, later.[4]

61. 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. 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.

62. What is more, it is no easy task to change or cancel a stolen Social Security number. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. In other words, preventive action to defend against the possibility of misuse of a Social Security number is not permitted; an individual must show evidence of actual, ongoing fraud activity to obtain a new number.

63. Even then, a new Social Security number may not be effective. According to the Identity Theft Resource Center: "The 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."[5]

64. Based on the foregoing, the information distributed in the Data Disclosure is significantly more valuable than the loss of, say, credit card information in a large retailer data

[4] *Identity Theft and Your Social Security Number*, Social Security Administration, http://www.ssa.gov/pubs/EN-05-10064.pdf (last visited July 24, 2020).
[5] 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-hackershas-millions-worrying-about-identity-theft.

disclosure. Victims affected by retailer breaches can avoid much of the potential future harm by cancelling credit or debit cards and obtaining replacements. By contrast, the information stolen in Presbyterian's Data Disclosure—including name, date of birth, Social Security number, and medical information—is difficult, if not impossible, to change.

65. Accordingly, this data demands a much higher price on the black market. As Martin Walter, senior director at cybersecurity firm RedSeal, explained, "Compared to credit card information, personally identifiable information and Social Security Numbers are worth more than 10x on the black market."[6]

66. It is also incorrect to assume that reimbursing a consumer for financial loss due to fraud makes that individual whole again. To the contrary, the U.S. Department of Justice's Bureau of Justice Statistics found that "among victims who had personal information used for fraudulent purposes, 29% spent a month or more resolving problems" and that "resolving the problems caused by identity theft [could] take more than a year for some victims."[7]

67. Fraudulent activity resulting from the Data Disclosure may not come to light for years. Despite all of the publicly available knowledge of the continued compromises of PHI and the dangers associated therewith, Presbyterian's approach to maintaining the privacy of its patients' PHI was lackadaisical, cavalier, reckless, or, at the very least, negligent.

68. Cyberattacks and data breaches at medical facilities like PHS are especially problematic because of the disruption they cause to the medical treatment and overall daily lives of patients affected by the attack.[8]

---

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

[7] Erika Harrel & Lynn Langton, *Victims of Identity Theft, 2012*, Bureau of Justice Statistics 10, 11 (Dec. 2013), https://www.bjs.gov/content/pub/pdf/vit12.pdf.

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

69. Indeed, researchers have found that at medical facilities that experienced a data security incident, the incident was associated with deterioration in timeliness and patient outcomes, generally.[9]

70. Similarly, cyberattacks and related data security incidents inconvenience patients. The various inconveniences patients encounter as a result of such incidents include, but are not limited to:

a. rescheduling medical treatment;

b. finding alternative medical care and treatment;

c. delaying or foregoing medical care and treatment;

d. undergoing medical care and treatment without medical providers having access to a complete medical history and records; and

e. losing patient medical history.[10]

71. Cyberattacks are considered a breach under the HIPAA Rules because there is an access to PHI that is not permitted under the HIPAA Privacy Rule and the access therefore constitutes "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."[11]

72. PHI and financial information are such valuable commodities to identity thieves that once the information has been compromised, criminals often trade the information on the "cyber black-market" for years.

---

[9] Sung J. Choi *et al*., *Data Breach Remediation Efforts and Their Implications for Hospital Quality*, WILEY ONLINE LIBRARY (Sept. 10, 2019), https://onlinelibrary.wiley.com/doi/full/10.1111/1475-6773.13203.
[10] Lisa Vaas, *Ransomware Attacks Paralyze, and Sometimes Crush, Hospitals* (Oct. 3, 2019), https://nakedsecurity.sophos.com/2019/10/03/ransomware-attacks-paralyze-and-sometimes-crush-hospitals/.
[11] *Id.*

73. 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 Class members are at an increased risk of fraud and identity theft for many years into the future. Thus, Plaintiffs and Class members must vigilantly monitor their financial and medical accounts for many years to come.

74. To date, Defendant has done absolutely nothing to provide Plaintiffs and the Class with relief for the damages they have suffered as a result of the Data Disclosure.

75. Presbyterian has failed to provide compensation to Plaintiffs and Class members victimized in this Data Disclosure. Presbyterian has not offered to provide any meaningful assistance or compensation for the costs and burdens—current and future—associated with identity theft and fraud resulting from the Data Disclosure. Presbyterian has not offered patients any assistance in dealing with the IRS or state tax agencies.

76. Presbyterian has also refused to offer credit monitoring for patients whose information was improperly disclosed. Therefore, the harm Plaintiffs and other patients face as a result of the Data Disclosure is compounded, as Presbyterian has declined to offer services that would help Plaintiffs and other patients protect against the heightened risk of identity theft and fraud that they now face. Instead, Plaintiffs and other patients bear the full burden of protecting against the heightened risk of identity theft and fraud caused by Presbyterian's Data Disclosure, including the substantial time and costs associated with such protective measures.

77. Accordingly, Plaintiff Gonzales has taken proactive measures to mitigate further access to his PII by purchasing an identity theft service package. On May 4, 2020, Plaintiff Gonzales purchased Identity Guard's premier family plan for an annual fee of $349.99.

78. The notification letter advises Plaintiffs and the Class to review statements from their health plan and providers for evidence of fraud or identity theft.

79. As a direct result of Presbyterian's failure to prevent the Data Disclosure, Plaintiffs have spent, and will continue to spend, time and effort attempting to mitigate the dangers and continuous risk of identity theft and tax fraud resulting from the disclosure of their PHI.

80. As a result of the Data Disclosure, the security and value of Plaintiffs' PHI has decreased. Plaintiffs have spent and will continue to have to spend hours monitoring their accounts for unauthorized activity.

81. The Data Disclosure also puts Plaintiffs at risk of the imminent and impending injury flowing from fraud and identity theft posed by their PHI being placed in the hands of unauthorized third parties.

82. Unless Presbyterian undertakes measures necessary to adequately protect Plaintiffs' PHI, which is still in Presbyterian's possession, Plaintiffs are also at risk of further breaches.

83. Plaintiffs and other Class members have suffered and will continue to suffer damages, including monetary losses, lost time, anxiety, and emotional distress. They have suffered or are at increased risk of suffering:

a. The loss of the opportunity to control how their PHI is used;

b. The diminution in value of their PHI;

c. The compromise, publication and theft of their PHI;

d. Out-of-pocket costs associated with the prevention, detection, recovery, and remediation from identity theft or fraud;

e. Lost opportunity costs and lost wages associated with effort expended and the loss of productivity from addressing and attempting to mitigate the actual and future consequences of the Data Disclosure, including, but not limited to, efforts spent researching how to prevent, detect, contest, and recover from identity theft and fraud;

f. Unauthorized use of stolen PHI;

g. Delay in receipt of tax refund monies;

h. The continued risk to their PHI, which remains in the possession of Presbyterian and is subject to further unauthorized distribution so long as Presbyterian fails to undertake appropriate measures to protect the PHI in its possession; and

i. Current and future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, remediate, and repair the impact of the Data Disclosure for the remainder of Plaintiffs and Class members' lives.

84. Plaintiffs and the Class have been or will be forced to spend time, energy, and money remedying or mitigating the effects of the Data Disclosure relating to:

a. Identifying and correcting fraudulent charges;

b. Canceling and reissuing credit and debit cards;

c. Purchasing credit monitoring and identity theft prevention;

d. Addressing their inability to withdraw funds linked to compromised accounts;

e. Taking trips to banks and waiting in line to obtain funds held in limited accounts;

f. Placing "freezes" and "alerts" with credit reporting agencies;

g. Spending time on the phone with or at a financial institution to dispute fraudulent charges;

h. Contacting financial institutions and closing or modifying financial accounts;

i. Resetting automatic billing and payment instructions from compromised credit and debit cards to new ones;

j. Paying late fees and declined payment fees imposed as a result of failed automatic payments that were tied to compromised cards that had to be cancelled; and

k. Closely reviewing and monitoring bank accounts and credit reports for unauthorized activity for years to come.

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

CLASS ACTION ALLEGATIONS

86. Plaintiffs bring this action on behalf of themselves and as a class action on behalf of the following proposed class:

> All individuals whose personal health information was compromised in the phishing attack discovered by Presbyterian Healthcare Services on June 6, 2019.

87. Excluded from the Class are the officers, directors, and legal representatives of Presbyterian and the judges and court personnel in this case and any members of their immediate families.

88. This action is properly maintainable as a class action under New Mexico Rule 1-023.

89. Numerosity. The members of the Class are so numerous that joinder of all members is impractical. Based on information and belief, the Class is estimated to include approximately 183,370 individuals. The exact number is generally ascertainable by appropriate discovery as Presbyterian has knowledge of the patients' whose PHI was improperly distributed.

90. 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 and to what extent Presbyterian had a duty to protect the PHI of Plaintiffs and the Class;

b. Whether Presbyterian failed to adopt the practices and procedures necessary to adequately safeguard the information compromised in the Data Disclosure;

c. Whether Presbyterian adequately and accurately informed Class Members that their PHI had been compromised;

d. Whether Class Members are entitled to actual damages and/or punitive damages as a result of Presbyterian's wrongful conduct; and

e. Whether Plaintiffs and the Class are entitled to restitution as a result of Presbyterian's wrongful conduct.

91. Typicality. Plaintiffs' claims are typical of those of other Class members because Plaintiffs' PHI, like that of every other Class member, was compromised by the Data Disclosure. Further, Plaintiffs, like all Class members, were injured by Presbyterian's uniform conduct. Plaintiffs are advancing the same claims and legal theories on behalf of themselves and all other Class members, and there are no defenses that are unique to Plaintiffs. The claims of Plaintiffs and those of other Class members arise from the same operative facts and are based on the same legal theories.

92. Adequacy of Representation. Plaintiffs will fairly and adequately represent and protect the interests of the Class in that they have no disabling conflicts of interest that would be antagonistic to those of the other members of the Class. The damages and infringement of rights

Plaintiffs suffered are typical of other Class members, and Plaintiffs seek no relief that is antagonistic or adverse to the members of the Class. Plaintiffs have retained counsel experienced in complex consumer class action litigation, and Plaintiffs intend to prosecute this action vigorously.

93. Superiority of Class Action. A class action is superior to other available methods for the fair and efficient adjudication of this controversy, as the pursuit of numerous individual lawsuits would not be economically feasible for individual Class members, and certification as a class action will preserve judicial resources by allowing the Class's common issues to be adjudicated in a single forum, avoiding the need for duplicative hearings and discovery in individual actions that are based on an identical set of facts. In addition, without a class action, it is likely that many members of the Class will remain unaware of the claims they may possess.

94. The litigation of the claims brought herein is manageable. Presbyterian's uniform conduct, the consistent provisions of the relevant laws, and the ascertainable identities of Class members demonstrates that there would be no significant manageability problems with prosecuting this lawsuit as a class action.

95. Adequate notice can be given to Class members directly using information maintained in Presbyterian's records.

96. Predominance. The issues in this action are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include but are not limited to the common questions of fact and law identified above.

97. This proposed class action does not present any unique management difficulties.

FIRST CAUSE OF ACTION
Negligence

(On Behalf of Plaintiffs and the Class)

98. Plaintiffs restate and re-allege all preceding paragraphs as if fully set forth herein.

99. Upon seeking treatment at Presbyterian, patients were obligated to provide Presbyterian with certain PHI, including their names, dates of birth, Social Security numbers, and health information. Presbyterian had full knowledge of the sensitivity of the PHI its patients provided and the types of harm that Plaintiffs and Class members could and would suffer if their PHI were wrongfully disclosed.

100. Presbyterian had a duty to exercise reasonable care in safeguarding, securing, and protecting such information from being compromised, lost, stolen, misused, and/or disclosed to unauthorized parties. This duty includes, among other things, designing, maintaining, and testing Presbyterian's policies regarding the storage, utilization, and distribution of patients' PHI to ensure that Plaintiffs and Class members' information was adequately secured and protected.

101. Plaintiffs and Class members were the foreseeable and probable victims of Presbyterian's inadequate security practices and procedures. Presbyterian knew or should have known of the inherent risks in collecting and storing PHI and the critical importance of providing adequate security for that PHI. Presbyterian also knew or should have known that it had inadequate employee training, education, and information security protocols in place to secure the PHI of Plaintiffs and the Class.

102. Presbyterian's conduct created a foreseeable risk of harm to Plaintiffs and Class members.

103. Presbyterian's misconduct included, but was not limited to, its failure to take the steps necessary to prevent the Data Disclosure as set forth herein and Presbyterian's decision not

to comply with industry standards for the safekeeping and use of the PHI of Plaintiffs and Class members.

104. Plaintiffs and the Class members had no ability to protect their PHI that was in Presbyterian's possession. Only Presbyterian was able to protect against the harm Plaintiffs and Class members suffered as a result of the Data Disclosure.

105. Presbyterian had and continues to have a duty to adequately notify Plaintiffs and Class members that their PHI was compromised, how it was compromised, and other details of the Data Disclosure. Such notice is necessary to allow Plaintiffs and the Class members to take steps to prevent, mitigate, and repair any identity theft or fraudulent use of their PHI by unauthorized third parties.

106. Presbyterian has failed to adequately notify Plaintiffs and the Class of the Data Disclosure, as the notification letter did not contain sufficient information detailing the incident, including, but not limited to, key information regarding the nature of the phishing incident and how the unauthorized third party obtained access to Plaintiffs' and Class members' PHI.

107. Presbyterian had a duty to have appropriate procedures in place to prevent the unauthorized dissemination of the PHI of Plaintiffs and Class members.

108. Presbyterian has acknowledged that the privacy and security of Plaintiffs' and Class members' PHI was compromised as a result of the Data Disclosure.

109. Presbyterian, through its actions and/or omissions, unlawfully breached its duty to Plaintiffs and the Class by failing to exercise reasonable care in protecting and safeguarding their PHI.

110. Presbyterian deviated from standard industry rules, regulations, and practices by improperly and inadequately safeguarding the Plaintiffs' and Class members' PHI.

111. Presbyterian, through its actions and/or omissions, unlawfully breached its duty to Plaintiffs and the Class by failing to have appropriate procedures in place to store and access patients' PHI and to detect and prevent unauthorized access to patients' PHI.

112. Presbyterian, through its actions and/or omissions, unlawfully breached its duty to timely and adequately disclose to Plaintiffs and Class members the existence and scope of the Data Disclosure.

113. But for Presbyterian's wrongful and negligent breach of these duties, Plaintiffs and Class members' PHI would not have been compromised.

114. There is a close causal connection between Presbyterian's failure to implement security measures to protect patients' PHI and the risk of imminent harm suffered by Plaintiffs and the Class.

115. As a result of Presbyterian's negligence, Plaintiffs and the Class have suffered and will continue to suffer damages and injury including, but not limited to, the increased risk of future identity theft and fraud, the costs associated therewith, and lost time spent monitoring, addressing, and correcting the current and future consequences of the Data Disclosure.

SECOND CAUSE OF ACTION
Intrusion Upon Solitude / Invasion of Privacy
(On Behalf of Plaintiffs and the Class)

116. Plaintiffs restate and re-allege all preceding paragraphs as if fully set forth herein.

117. The State of New Mexico recognizes the tort of invasion of privacy, comprised of four sub-torts including intrusion upon solitude (seclusion), and adopts the formulation of that tort found in the Restatement (Second) of Torts, which states:

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

Restatement (Second) of Torts § 652B (1977).

118. Plaintiffs and Class members had a legitimate expectation of privacy to their PHI and were entitled to the protection of this information against disclosure to unauthorized third parties.

119. Presbyterian owed a duty to its patients, including Plaintiffs and Class members, to keep their PHI confidential.

120. Presbyterian permitted unauthorized third parties to access the PHI of Plaintiffs and Class members.

121. Presbyterian's conduct as alleged above intruded upon Plaintiffs' and Class members' seclusion under common law.

122. The unauthorized release to, custody of, and examination by unauthorized third parties of the PHI of Plaintiffs and Class members, especially where the information includes Social Security numbers and health information, would be highly offensive to a reasonable person.

123. The intrusion was into a place or thing, which is private and is entitled to be private. Plaintiffs and Class members disclosed their PHI to Presbyterian as part of their medical treatment but did so privately and with the intention that the PHI would be kept confidential and would be protected from unauthorized disclosure.

124. Plaintiffs and Class members were reasonable to believe that their PHI would be kept private and would not be disclosed without their authorization.

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

126. As a proximate result of Presbyterian's acts and omissions, the PHI of Plaintiffs and the Class was disclosed to unknown third parties without authorization, causing Plaintiffs and Class members to suffer damages.

127. Unless and until enjoined and restrained by order of this Court, Presbyterian's wrongful conduct will continue to cause great and irreparable injury to Plaintiffs and Class members in that the PHI entrusted to Presbyterian can be viewed, distributed, and used by unauthorized persons. Plaintiffs and Class members have no adequate remedy at law for the injuries they suffered, as a judgment for monetary damages will not end the invasion of privacy for Plaintiffs and the Class.

THIRD CAUSE OF ACTION
Breach of Express Contract
(On Behalf of Plaintiffs and the Class)

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

129. Plaintiffs and Members of the Class allege that they entered into valid and enforceable express contracts or were third party beneficiaries of valid and enforceable express contracts, with Defendant.

130. The valid and enforceable express contracts that Plaintiffs and Class Members entered into with Defendant include Defendant's promise to protect nonpublic personal information given to Defendant or that Defendant gathers on its own from disclosure.

131. Under these express contracts, Defendant and/or its affiliated healthcare providers, promised and were obligated to: (a) provide healthcare to Plaintiffs and Class Members; and (b) protect Plaintiffs' and the Class members' PHI: (i) provided to obtain such healthcare; and/or (ii)

created as a result of providing such healthcare. In exchange, Plaintiffs and Members of the Class agreed to pay money for these services.

132. Both the provision of healthcare and the protection of Plaintiffs' and Class Members' PII/PHI were material aspects of these contracts.

133. At all relevant times, Defendant expressly represented in its Notice of Privacy Practices that it was required by law: (i) to "maintain the privacy of your health information;" (ii) to inform and notify patients "when your protected health information has been inappropriately accessed, used, or disclosed as a result of a breach"; and (iii) to not "use or share your health information without your written authorization unless required by law or as described in this Joint Notice of Privacy Practices." Ex. C at 1, 3. Defendant further expressly represented in its Patient Rights document that its patients, including Plaintiffs and Class members, have a right to confidentiality of medical records and personal information.

134. Defendant's express representations, including, but not limited to, express representations found in its Notice of Privacy Practices, formed an express contract requiring Presbyterian to implement data security adequate to safeguard and protect the privacy of Plaintiffs' and Class members' PHI.

135. Consumers of healthcare value their privacy, the privacy of their dependents, and the ability to keep their PHI private. To customers such as Plaintiffs and Class members, healthcare that does not adhere to industry standard data security protocols to protect PHI is fundamentally less useful and less valuable than healthcare that adheres to industry-standard data security. Plaintiffs and Class members would not have entered into contracts with Presbyterian and/or its affiliated healthcare providers without an understanding that their PHI would be safeguarded and protected.

136. A meeting of the minds occurred, as Plaintiffs and members of the Class provided their PHI to Presbyterian and/or its affiliated healthcare providers, and paid for the provided healthcare in exchange for, amongst other things, protection of their PHI.

137. Plaintiffs and Class members performed their obligations under the contract when they paid for their health care services.

138. Defendant materially breached their contractual obligation to protect the nonpublic personal information Presbyterian gathered when the information was accessed and exfiltrated by unauthorized personnel as part of the Data Disclosure.

139. Presbyterian materially breached the terms of these express contracts, including, but not limited to, the terms stated in the relevant Notice of Privacy Practices. Presbyterian did not "maintain the privacy" of Plaintiffs' and Class members' PHI as evidenced by its notifications of the Data Disclosure to Plaintiffs and approximately 183,000 Class members. Specifically, Presbyterian did not comply with industry standards, or otherwise protect Plaintiffs' and the Class Members' PHI, as set forth above.

140. The Data Disclosure was a reasonably foreseeable consequence of Presbyterian's actions in breach of these contracts.

141. As a result of Presbyterian's failure to fulfill the data security protections promised in these contracts, Plaintiffs and members of the Class did not receive the full benefit of the bargain, and instead received healthcare and other services that were of a diminished value to that described in the contracts. Plaintiffs and Class members therefore were damaged in an amount at least equal to the difference in the value of the healthcare with data security protection they paid for and the healthcare they received.

142. Had Presbyterian disclosed that its security was inadequate or that it did not adhere to industry-standard security measures, neither the Plaintiffs, the Class members, nor any reasonable person would have purchased healthcare from Presbyterian and/or its affiliated healthcare providers.

143. As a direct and proximate result of the Data Disclosure, Plaintiffs and Class members have been harmed and have suffered, and will continue to suffer, actual damages and injuries, including without limitation the release, disclosure, and publication of their PHI, the loss of control of their PHI, the imminent risk of suffering additional damages in the future, disruption of their medical care and treatment, out-of-pocket expenses, and the loss of the benefit of the bargain they had struck with Presbyterian.

144. Plaintiffs and Class members are entitled to compensatory and consequential damages suffered as a result of the Data Disclosure.

FOURTH CAUSE OF ACTION
Breach of Implied Contract
(On Behalf of Plaintiffs and the Class)

145. Plaintiffs restate and re-allege all preceding paragraphs as if fully set forth herein.

146. Plaintiffs and Class members were required to provide their PHI—including names, dates of birth, Social Security numbers, and medical information—to Presbyterian as a condition of their treatment.

147. Implicit in the agreement between Presbyterian and its patients was the obligation that both parties would maintain information confidentially and securely.

148. Presbyterian had an implied duty of good faith to ensure that the PHI of Plaintiffs and Class members in its possession was only used to provide medical treatment, billing, and other medical benefits from Presbyterian.

149. Presbyterian had an implied duty to reasonably safeguard and protect the PHI of Plaintiffs and Class members from unauthorized disclosure or uses.

150. Additionally, Presbyterian implicitly promised to retain this PHI only under conditions that kept such information secure and confidential.

151. Plaintiffs and Class members fully performed their obligations under the implied contract with Presbyterian. Presbyterian did not. Plaintiffs and Class members would not have provided their confidential PHI to Presbyterian in the absence of their implied contracts with Presbyterian and would have instead retained the opportunity to control their PHI for uses other than medical treatment, billing, and benefits from Presbyterian.

152. Presbyterian breached the implied contracts with Plaintiffs and Class members by failing to reasonably safeguard and protect Plaintiffs and Class members' PHI, which was compromised as a result of the Data Disclosure.

153. Presbyterian's acts and omissions have materially affected the intended purpose of the implied contacts requiring Plaintiffs and Class members to provide their PHI as a condition of employment in exchange for medical treatment and benefits.

154. As a direct and proximate result of Presbyterian's breach of its implied contacts with Plaintiffs and Class members, Plaintiffs and Class members have suffered and will suffer injury, including but not limited to: (i) the loss of the opportunity to control how their PHI is used; (ii) the compromise, publication, and/or theft of their PHI; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PHI; (iv) lost opportunity costs associated with effort expended and the loss of productivity caused by addressing and attempting to mitigate the actual and future consequences of the Data Disclosure, including but not limited to efforts spent researching how to prevent, detect, contest

and recover from tax fraud and identity theft; (v) costs associated with placing freezes on credit reports; (vi) the continued risk to their PHI, which remains in Presbyterian's possession and is subject to further unauthorized disclosures so long as Presbyterian fails to undertake appropriate and adequate measures to protect the PHI of current and former patients that is in its 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 PHI compromised as a result of the Data Disclosure for the remainder of the lives of Plaintiffs and Class members.

FIFTH CAUSE OF ACTION
NEGLIGENCE PER SE
(On Behalf of Plaintiffs and the Class)

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

140. Pursuant to the Federal Trade Commission Act (15 U.S.C. § 45), Presbyterian had a duty to provide fair and adequate computer systems and data security practices to safeguard Plaintiffs' and Class members' PHI.

141. Pursuant to HIPAA (42 U.S.C. § 1302d, et seq.), Presbyterian had a duty to implement reasonable safeguards to protect Plaintiffs' and Class members' PHI.

142. Pursuant to HIPAA, Presbyterian had a duty to render the electronic PHI it maintained unusable, unreadable, or indecipherable to unauthorized individuals, 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.

143. Pursuant to the Gramm-Leach-Bliley Act, 15 U.S.C. § 6801, Presbyterian had a duty to protect the security and confidentiality of Plaintiffs' and Class Members' PHI.

144. Presbyterian breached its duties to Plaintiffs and Class members under the Federal Trade Commission Act, HIPAA, and the Gramm-Leach-Bliley Act by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiffs' and Class members' PHI.

145. Presbyterian's failure to comply with applicable laws and regulations constitutes negligence per se.

146. But for Presbyterian's wrongful and negligent breach of its duties owed to Plaintiffs and Class members, Plaintiffs and Class members would not have been injured.

147. The injury and harm suffered by Plaintiffs and Class members was the reasonably foreseeable result of Presbyterian's breach of its duties. Presbyterian knew or should have known that it was failing to meet its duties, and that Presbyterian's breach would cause Plaintiffs and Class members to experience the foreseeable harms associated with the exposure of their PHI.

148. As a direct and proximate result of Presbyterian's negligent conduct, Plaintiffs and Class members have suffered injury and are entitled to compensatory, consequential, and punitive damages in an amount to be proven at trial.

SIXTH CAUSE OF ACTION
Breach of Fiduciary Duty
(On Behalf of Plaintiffs and the Class)

155. Plaintiffs restate and re-allege all preceding paragraphs as if fully set forth herein.

156. Presbyterian, as a medical provider, was a fiduciary and was required to act primarily for the benefit of its patients, including Plaintiffs and Class members, for the safeguarding of patients' PHI.

157. Presbyterian had a fiduciary duty to act on the benefit of Plaintiffs and Class members upon matters within the scope of their provider/patient relationship, in particular to keep secure the medical information and the PHI of Presbyterian's patients.

158. Presbyterian breached its duty of care to Plaintiffs and Class members by allowing third parties to access Plaintiffs and Class members' PHI and medical information without authorization and/or for improper purposes and by failing to provide adequate protections to its patients' PHI.

159. As a direct and proximate result of Presbyterian's actions alleged above, the Plaintiffs and Class members have suffered damages.

SEVENTH CAUSE OF ACTION
VIOLATION OF THE NEW MEXICO UNFAIR PRACTICES ACT
(NMSA 1978, Section 57-12-2)
(On Behalf of Plaintiffs and the Class)

160. Plaintiffs re-allege and incorporate by reference the paragraphs above as if fully set forth herein.

161. By the acts and conduct alleged herein, Defendant committed unfair or deceptive acts and practices by:

a. failing to maintain adequate computer systems and data security practices to safeguard PHI;

b. failing to disclose that its computer systems and data security practices were inadequate to safeguard PHI from theft;

c. continued gathering and storage of PHI and other personal information after Defendant knew or should have known of the security vulnerabilities of its computer systems that were exploited in the phishing incident and Data Disclosure;

d. making and using false promises, set out in the Presbyterian Privacy Notice and Patient Rights, about the privacy and security of PHI of Plaintiffs and Class Members;

e. deceptively misrepresenting the true nature and character of Presbyterian's data security practices; and

f. continued gathering and storage of PHI and other personal information after Presbyterian knew or should have known of the cyberattack and Data Disclosure and before Defendant allegedly remediated the data security incident.

162. These unfair acts and practices violated duties imposed by laws, including but not limited to, the Federal Trade Commission Act, HIPAA, the Gramm-Leach-Bliley Act, and the New Mexico Unfair Practices Act.

163. Presbyterian is a "person" engaged in "trade or commerce," as defined in the New Mexico Unfair Practices Act, NMSA 1978, Section 57-12-2.

164. Presbyterian has committed an unfair or deceptive trade practice as that term is defined in the New Mexico Unfair Practices Act, NMSA 1978 §§ 57-12-2(D). The provisions violated by Defendant include, but are not limited to, the following:

a. "unfair or deceptive trade practice" means any false or misleading oral or written statement, visual description or other representation of any kind knowingly made in connection with the sale, lease, rental or loan of goods or services or in the extension of credit or in the collection of debts by any person in the regular course of his trade or commerce, which may, tends to or does deceive or mislead any person and includes but is not limited to:

i. causing confusion or misunderstanding as to the source, sponsorship, approval or certification of goods or services;

ii. deceptive representations or designations of geographic origin in connection with goods or services;

iii. offering goods or services with intent not to supply reasonable expectable public demand;

iv. using exaggeration, innuendo, or ambiguity as to a material fact or failing to state a material fact if doing so deceives or tends to deceive; and

v. failing to deliver the quality or quantity of goods or services contracted for.

165. The acts and omissions of said Presbyterian were done knowingly and intentionally with the purpose of the sale of goods and services to the Plaintiffs and Class members.

166. Plaintiffs and Class members were injured because: (a) they would not have purchased medical care and treatment from Presbyterian had they known the true nature and character of Presbyterian's data security practices; (b) Plaintiffs and Class members would not have entrusted their PHI to Presbyterian in the absence of promises that Presbyterian would keep their information reasonably secure, and (c) Plaintiffs and Class members would not have entrusted their PHI to Presbyterian in the absence of the promise to monitor its computer systems and networks to ensure that it adopted reasonable data security measures.

167. As a direct and natural consequence of the violation of the Unfair Practices Act, Plaintiffs and Class members suffered injury and all the other damages including, but not limited to: (i) actual identity theft; (ii) the compromise, publication, and/or theft of their PHI; (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 Disclosure, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (v) the continued risk to their PHI, which remains in Presbyterian's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PHI in its continued possession; (vi) future costs in terms of time, effort, and money that will be expended as result of the Data Disclosure for the remainder of the lives of Plaintiffs and Class members; and (vii) the diminished value of Presbyterian's services they received.

168. Plaintiffs and Class members are also entitled to statutory damages in the sum of $100 per person, if that amount is greater than the actual damages sustained.

169. It has become necessary for Plaintiffs to employ attorneys for purposes of representing them herein, and therefore, are entitled to recover their attorneys' fees pursuant to Section 39-2-1 NMSA 1978 and treble damages pursuant to § 57-12-10 (B), (C) and (D) NMSA 1978.

170. Under § 57-12-10 NMSA (1978) Plaintiffs and Class members are entitled to an award of up to three times the actual damages should they so elect, as opposed to punitive damages, which are also available under the facts of this case. Plaintiffs and Class members are also entitled to an award of reasonable attorneys' fees in connection with the prosecution of these claims.

PRAYER FOR RELIEF

WHEREFORE Plaintiffs on behalf of themselves and all others similarly situated, request the following relief:

A. An Order certifying this action as a class action and appointing Plaintiffs as Class representatives and their counsel as Class counsel;

B. A mandatory injunction directing Presbyterian to hereinafter adequately safeguard the PHI of Plaintiffs and the Class by implementing improved security procedures and measures;

C. A mandatory injunction requiring that Presbyterian provide notice to each member of the Class relating to the full nature and extent of the Data Disclosure and the disclosure of PHI to unauthorized persons;

D. An award of actual damages, compensatory damages, statutory damages, and statutory penalties, in an amount to be determined;

E. For an award of punitive damages, as allowable by law;

F. An award of attorneys' fees and costs;

G. An award of pre- and post-judgment interest, costs, attorneys' fees, expenses, and interest as permitted by law; and

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

DEMAND FOR JURY TRIAL

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

Dated: August 11, 2020

Respectfully submitted,

/s/ Lincoln Combs

Lincoln Combs
1239 Paseo de Peralta
Santa Fe, New Mexico 87501
2575 E. Camelback Rd., Suite 1100
Phoenix, Arizona 85016
Telephone: (602) 530-8000
Facsimile: (602) 530-8500
lincoln.combs@gknet.com

Lynn A. Toops (*pro hac vice* forthcoming)
Lisa M. La Fornara (*pro hac vice* forthcoming)
COHEN & MALAD, LLP

One Indiana Square, Suite 1400
Indianapolis, IN 46204
Telephone: (317) 636-6481
Facsimile: (317) 636-2593
ltoops@cohenandmalad.com
llafornara@cohenandmalad.com

Gerard Stranch, IV (*pro hac vice* forthcoming)
BRANSTETTER, STRANCH
& JENNINGS, PLLC
223 Rosa Parks Avenue, Suite 200
Nashville, Tennessee 37203
Telephone: (615) 254-8801
Facsimile: (615) 255-5419
gerards@bsjfirm.com

Alyson S. Beridon (*pro hac vice* forthcoming)
BRANSTETTER, STRANCH
& JENNINGS, PLLC
425 Walnut Street, Suite 2315
Cincinnati, Ohio 45202
Telephone: (513) 381-2224
Facsimile: (615) 255-5419
alysonb@bsjfirm.com

Christopher D. Jennings (*pro hac vice* forthcoming)
JOHNSON FIRM
610 President Clinton Avenue, Suite 300
Little Rock, Arkansas 72201
Telephone: 501-372-1300
Facsimile: 888-505-0909
chris@yourattorney.com

Jesse S. Johnson
GREENWALD DAVIDSON RADBIL PLLC
7601 N. Federal Hwy., Suite A-230
Boca Raton, Florida 33587
Telephone: (561) 826-5477
jjohnson@gdrlawfirm.com

Gary M. Klinger (*pro hac vice forthcoming*)
Kozonis & Klinger, Ltd.
227 W. Monroe Street, Suite 2100
Chicago, Illinois 60630
Telephone: (312) 283-3814
Facsimile: 773-496-8617
gklinger@kozonislaw.com

Todd S. Garber (*pro hac vice forthcoming*)
Jeremiah Frei-Pearson (*pro hac vice forthcoming*)
Chantel R. Mills (*pro hac vice forthcoming*)
FINKELSTEIN, BLANKINSHIP, FREI-PEARSON & BARBER, LLP
One North Broadway, Suite 900
White Plains, New York 10601
Tel: (914) 298-3283
Fax: (914) 298-4383
tgarber@fbfglaw.com
jfrei-pearson@fbfglaw.com
cmills@fbfglaw.com

Kristina Martinez
EGOLF + FERLIC +
MARTINEZ + HARWOOD, LLC
123 West San Francisco Street, Second Floor
Santa Fe, New Mexico 87501
Tel: (505) 986-9641
Fax: (505) 214-2005
kmartinez@EgolfLaw.com

Counsel for the Plaintiffs and the Proposed Class

Exhibit A

PRESBYTERIAN
C/O ID Experts
Return Mail Processing Center
P.O. Box 6336
Portland, OR 97228-6336

Please Call ID Experts with Questions:
(833) 297-6405

4887001018577
000 0004181 00000000 0001 0001 04181 INS: 0 0
KYRA M NIETO
[redacted]

November 25, 2019

Dear Kyra M Nieto:

At Presbyterian, we are committed to protecting the privacy of our patients and members. You are receiving this letter because you have received health care services through a Presbyterian provider and/or you have been a Presbyterian Health Plan member.

On June 6, 2019, Presbyterian discovered anonymous, unauthorized access gained through a deceptive email to some of Presbyterian's workforce members around May 9, 2019. We believe that the unauthorized access to these email accounts was part of a scam or deceptive email trying to get information, known as "phishing." There was no access to the health record system or any other systems. Upon discovering the issue on June 6, 2019, Presbyterian secured the email accounts, alerted federal law enforcement, and began conducting thorough review of these email accounts.

As a result of Presbyterian's ongoing investigation and review, we determined on November 14, 2019, that certain affected email accounts included data containing your name and might have contained your date of birth, clinical and/or health insurance information. We are not aware of any improper or attempted use of your information, but we believe it important to notify you of this incident. We are very sorry that this incident occurred and for any concern it causes.

We take the responsibility of safeguarding your information very seriously. All workforce members must successfully complete annual mandatory training about the importance and requirement to safeguard all information.

We recommend that you review the statements that you receive from your health plan or your health care providers regarding your health care services. If you see any service that you believe you did not receive, please contact the health plan or provider immediately.

We want to assure you that Presbyterian is committed to protecting the privacy and confidentiality of every individual's information, and we continue to take steps to enhance the security of our systems as part of this commitment.

If you have any questions, please call (833)297-6405, Monday through Friday, 7:00 a.m. to 7:00 p.m. Mountain Time.

Sincerely,

Sophia Collaros
Privacy Officer

Exhibit B

PRESBYTERIAN

Notification of Data Security Incidents

At Presbyterian, we are committed to protecting the privacy of our patients and members.

On June 6, 2019, Presbyterian discovered anonymous, unauthorized access was gained through a deceptive email to some of Presbyterian's workforce members sometime around May 9, 2019. Presbyterian believes that the unauthorized access to these email accounts was part of a "phishing" scam trying to get information. These email accounts included patient and/or health plan member names and might have contained dates of birth, Social Security numbers and clinical and/or health plan information. Once Presbyterian became aware of this incident, it secured these email accounts, began a thorough review of the impacted emails and alerted federal law enforcement.

We are very sorry that unauthorized access to some of the workforce members' emails occurred. We are not aware of any improper use, or attempted use of your information, but we believe it is important to notify you of this incident. This did not affect our electronic health records or billing systems.

We take the responsibility of safeguarding your information very seriously. To help prevent this incident from happening again, Presbyterian is taking several steps and implementing additional security measures to further protect our email system. In addition, all workforce members annually must successfully complete mandatory training about the importance and requirement to safeguard all information. In particular, workforce members have received, and will continue to receive, reminders about safeguarding information stored electronically and how to avoid phishing scams.

We recommend that you review the statements that you receive from your health plan or your health care providers regarding your health care services. If you see any service that you believe you did not receive, please contact the health plan or provider immediately. We want to assure you

that Presbyterian is committed to protecting the privacy and confidentiality of every individual's information.

If you have any questions, please call 1-833-297-6405, Monday through Friday, 7:00 a.m. to 7:00 p.m. Mountain Time.

Aviso de Incidente de Seguridad de Datos

Update on Previously Announced Personally Identifiable Information Incident

Presbyterian mailed additional letters to some individual providers in the Presbyterian Health Plan network, including Presbyterian-employed providers, regarding the previously announced phishing incident.

On July 31, 2019, Presbyterian learned that an unauthorized person may have accessed some employee email accounts through a "phishing" scam. Once Presbyterian became aware of this incident, it secured the affected email accounts and alerted federal law enforcement. At least one of these email accounts contained provider names and Social Security numbers.

While Presbyterian's investigation remains ongoing at this time, there is no evidence indicating that any of the providers' information was downloaded or used in any way.

Presbyterian is offering providers complimentary credit monitoring. Presbyterian also established a dedicated call center to answer questions for those affected by this incident.

To help prevent this type of incident from happening again, Presbyterian has implemented additional security measures to further protect our email system. In addition, all employees complete annual training related to protecting all information.

Presbyterian regrets that this incident occurred and has services and support in place to help affected individuals. Providers who have questions can call 1-833-959-1350, Monday through Friday, 7 a.m. to 7 p.m. Mountain time. If you are a provider and believe you may have been affected, but did not receive a letter, please contact the call center to verify information.

FINANCIAL ASSISTANCE AND COVERING YOUR CARE AT A PRESBYTERIAN FACILITY

COMMUNITY HEALTH ASSESSMENT IMPLEMENTATION PLANS

DOCTORS & SERVICES

Quick Care

Presbyterian Medical Group Directory

PHS Coordinated Care

Covering Your Care & Financial Assistance

About Our Quality Doctors

PMG Urgent Care & Clinic Locations

Services & Centers

HOSPITALS

Presbyterian Hospital

Presbyterian Kaseman Hospital

Presbyterian Rust Medical Center

Presbyterian Española Hospital

Dr. Dan C. Trigg Memorial Hospital

Socorro General Hospital

Lincoln County Medical Center

Plains Regional Medical Center

Presbyterian Santa Fe Medical Center

HEALTH PLANS

Individual & Family Plans

Medicare Advantage Plans

Centennial Care Medicaid Plans

Employer-Offered Plans

Understanding Health Insurance

TOOLS & RESOURCES

Patient Tools & Resources

Member Tools & Resources

COMMUNITY

About Presbyterian

Chaplaincy Services

Committed to Community Health

Legacy of Caring

Presbyterian Healthcare Foundation

Volunteer

For Job Seekers

For Providers

For Employers & Producers

Contact Us

Accessibility

Forms & Documents

Patient Rights

Member Rights

Employee Email

PresNet Login

About Presbyterian

Privacy & Security

Terms of Use

Nondiscrimination

Pharmaceutical Company Requests

Vendors

Exhibit C

OUR PRIVACY PRACTICES AND YOUR RIGHTS: JOINT NOTICE OF PRIVACY PRACTICES

This notice describes how medical information about you may be used and disclosed and how you can get access to this information. Please review it carefully.

The privacy practices of Presbyterian Healthcare Services ("Presbyterian") and certain organizations that participate in an organized health care arrangement ("OHCA") with Presbyterian are described in this *Joint Notice of Privacy Practices* ("Notice"). Health information about you is contained in our records, but the information in those records belongs to you. This Notice will help you understand how we protect the privacy of your health information and how to complain if you believe your privacy rights have been violated. The terms "we" and "our" used in this Notice refer to Presbyterian and the members of our OHCA that share this Notice and agree to abide by its terms.

HOW WE PROTECT THE PRIVACY OF YOUR HEALTH INFORMATION

Whenever possible, Presbyterian uses or shares health information that doesn't identify you. We have policies and procedures to protect the privacy of health information that does identify you. We have a training program to educate our employees and others about our privacy policies. Your health information is only used or shared for our business purposes or as otherwise required or allowed by law. When a service involving your health information is being performed by a third party, we require a written agreement with them to protect the privacy of your health information.

OUR RESPONSIBILITIES

- We are required by law to maintain the privacy of your health information.
- We are required to provide patients, except inmates, with this Notice that describes our legal duties and privacy practices regarding protected health information.
- We have a legal duty to notify you, and you have a right to know when your protected health information has been inappropriately accessed, used, or disclosed as a result of a breach.
- We must follow the terms of the most current *Joint Notice of Privacy Practice*, and are required to ask you for a written acknowledgement that you received a copy.

YOUR HEALTH INFORMATION RIGHTS

You have rights with respect to your protected health information. For more information on how to exercise these rights, see the *How to Make a Request* section of this Notice. The health information rights described in this Notice also apply to a person with legal authority to make health care decisions for a child or other person (for example, a parent or legal guardian). There are exceptions. For example, in New Mexico some health care services can be provided to a minor without the consent of a parent, guardian or other person. In these cases, the minor has the rights described in this Notice for health information related to the health care service provided. Some of the rights described here are subject to certain limitations and conditions.

Right to See and Get a Copy of Health Information. You have the right to see and get a copy of your health information. Usually, this information is contained in medical and billing records. You must make a request in writing to see or get a copy of your health information in our designated record set.

Right to Amend Incorrect or Incomplete Health Information. We strive to ensure that health information kept in our records is accurate and complete. However, occasionally a mistake can occur. You have the right to request that we change incorrect or incomplete health information in our records. We may deny your request if appropriate.

Right to Request Confidential Communications. You have the right to request that we deliver health information to you in a certain way or at a certain location. We must agree to a reasonable request or may deny your request if it is against the law or our policies.

Right to Request Restrictions of the Use or Disclosure of Your Health Information. You have the right to request that your health information is not used or shared for certain purposes. We are not required to agree to your request except if required by law, or if you request restriction to disclosure of your protected health information to the health plan and you pay Presbyterian for those services or health care items in full. We must tell you if we cannot agree to your request.

Right to Request an Accounting of Disclosures. You have the right to request an *Accounting of Disclosures*. This report will show when your health information was shared by us outside of our organization without your written authorization.

Right to Receive a Paper Copy of this Notice. You have a right to receive a paper copy of this Notice, even if you also agreed to receive it electronically.

WHEN HEALTH INFORMATION CAN BE USED OR SHARED WITHOUT A WRITTEN AUTHORIZATION

For Treatment. We use and share your health information to provide medical treatment to you by our health care providers.

For Payment. We use and share your health information in order to receive or facilitate payment for the treatment and services provided to you.

For Health Care Operations. We use and share health information in order to operate our business and deliver quality care and services to our patients.

Required by Law. We will use and share your health information when required by federal, state or local law.

Emergency Situations. We will use professional judgment to decide if sharing your health information is in your best interest during a health emergency or if you are incapacitated.

Public Health Activities. We share your health information with public health authorities to ensure the public welfare.

Health Oversight Activities. Your health information may be shared with health oversight agencies that have authority to monitor our activities.

Legal and Administrative Proceedings. Your health information may be shared as part of an administrative or legal proceeding.

Law Enforcement. If a law enforcement official requests, we may share only very limited health information.

Coroners, Medical Examiners and Funeral Directors. The health information of a deceased person may be shared with coroners, medical examiners and funeral directors so they can carry out their duties.

Organ and Tissue Donation. Your health information may be shared with organizations that obtain, store or transplant human organs and tissues.

Public Safety. Your health information may be shared to prevent or lessen a serious and immediate threat to the health or safety of anyone or the general public.

Special Government Functions. Your health information may be shared with federal officials for national security purposes authorized by law.

Correctional Institutions. If you are an inmate, your health information may be shared with correctional institutions or law enforcement officials in order to protect your health, or the health and safety of others.

Worker's Compensation. Your health information may be used or shared as required by worker's compensation laws.

Change of Ownership. If Presbyterian or any member of the OHCA that shares this Notice is sold or merged with another organization, records that contain your health information will become the property of the new owner.

Secretary of Health and Human Services. We are required by law to share health information with the Secretary of the U.S. Department of Health and Human Services (HHS) when HHS requests the health information to determine our compliance with privacy law.

WHEN A WRITTEN AUTHORIZATION IS REQUIRED TO USE OR SHARE HEALTH INFORMATION

We will not use or share your health information without your written authorization unless required by law or as described in this *Joint Notice of Privacy Practices*. You may cancel an authorization in writing at any time, except to the extent we have already taken action according to the authorization.

Marketing. We do not use or share your health information for marketing purposes without a written authorization from you. There are two exceptions that are permitted: when we have a face-to-face conversation with you or when we give you a promotional gift of little or no monetary value. If a marketing activity would involve any direct or indirect remuneration to us from a third party, the written authorization you would be asked to sign will state that fact.

Research. With your written authorization, we may share your health information with researchers conducting research that has been approved by Presbyterian's Institutional Review Board or another research/privacy board.

Sale of Protected Health Information. We do not sell your health information to anyone.

WHEN YOU MAY RESTRICT OR OPT OUT OF THE USE OR SHARING OF YOUR HEALTH INFORMATION

Facility Directory. Unless you object, we will use your name, your location in our facility, your general medical condition and your religious preference as directory information. Directory information may be shared with members of the clergy of your faith.

Notification and Communication with Family or Others Involved in Your Care. Unless you tell us that you object, we may share your health information with a person involved in your healthcare. If we do so, we may only share the information directly related to that person's involvement in your care or payment for your care.

Disaster Relief Activities. Unless you tell us that you object, we may use and share your health information with a public or private organization legally authorized to assist in disaster relief efforts so that your family can be notified about your condition, status and location.

Fundraising. We may contact you to raise funds for Presbyterian. The money raised is used for health care services and educational programs we provide to the community. Fundraising materials will describe your right to opt out of future fundraising. For more information see the *How to Make a Request* section of this Notice.

PREBYTERIAN'S RIGHT TO CHANGE THIS PRIVACY NOTICE

Presbyterian reserves the right to change the privacy practices described in this *Joint Notice of Privacy Practices* at any time. If the terms of this Notice should change, we will publish a new Notice and post it in our facilities and on our web site. It will be given to you upon request and as required by law. The terms described in the new Notice will apply to all health information maintained by Presbyterian and all members of the OHCA that share this Notice. You may obtain an electronic copy of this Notice from our web site at www.phs.org.

OTHER PARTICIPANTS IN OUR ORGANIZED HEALTH CARE ARRANGEMENT (OHCA)

The law allows members of an OHCA to share your health information with each other for certain purposes: for treatment, to receive payment for services, or for the health care operations of the OHCA. The following OHCA members have agreed to follow the privacy practices described in this *Joint Notice of Privacy Practices:*

- Presbyterian Healthcare Services – All facilities
- All facilities and clinics operated, leased or managed by Presbyterian
- Hospital-based physicians and groups who agree with Presbyterian to be subject to this Notice.
- Presbyterian Home Healthcare Services – All divisions

Presbyterian is also a member of an OHCA with Presbyterian Health Plan, Inc. and Presbyterian Insurance Company, Inc. which have their own Notice.

HOW TO MAKE A REQUEST: To request a copy of, an amendment to, or an *Accounting of Disclosures* of your health information from Presbyterian, you may contact Health Information Management at (505) 841-1740 or outside Albuquerque at 1-866-352-1528. To request that Fundraising materials not be sent to you, contact: Presbyterian Healthcare Foundation at (505) 724-6580. To file a complaint about our privacy practices, contact the Presbyterian Privacy Official at (505) 923-6176 or the Secretary of HHS, Office for Civil Rights, Region VI, 1301 Young Street, Suite 1169, Dallas, TX 75202. You will not be retaliated against for filing a complaint. For further information, contact Presbyterian's Compliance Dept. at (505) 923-8544.

Effective as of amendment date – August 1, 2013