Hart L. Robinovitch (AZ SBN 020910)
ZIMMERMAN REED LLP
14646 North Kierland Blvd., Suite 145
Scottsdale, AZ 85254
Telephone: (480) 348-6400
Facsimile: (480) 348-6415
Email: hart.robinovitch@zimmreed.com

Attorneys for Plaintiffs and the Class

(Additional Counsel listed below)

UNITED STATES DISTRICT COURT

DISTRICT OF ARIZONA

Angela T. Travis, Kerri G. Peters, and Geraldine Pineda, individually and on behalf of others similarly situated,

Plaintiffs,

v.

Assured Imaging, LLC, an Arizona limited liability company,

Defendant.

Case No.

CLASS ACTION COMPLAINT

JURY TRIAL DEMANDED

Plaintiffs ANGELA T. TRAVIS, KERRI G. PETERS, and GERALDINE PINEDA ("Plaintiffs"), individually and on behalf of all others similarly situated, bring this action against Defendant ASSURED IMAGING, LLC ("ASSURED" or "Defendant"), an Arizona domestic limited liability company, 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 the facts that are a matter of public record:

I. PARTIES

1. Plaintiff ANGELA T. TRAVIS is, and at all times mentioned herein was, an individual citizen of the State of Washington residing in Burien, Washington, and is a patient of Defendant ASSURED. Plaintiff Travis received notice of the data breach, and a copy of the notice is attached hereto as Exhibit A.

2. Plaintiff KERRI G. PETERS is, and at all times mentioned herein was, an individual citizen of the State of New Mexico, residing in Los Lunas, New Mexico, and is a patient of Defendant ASSURED. Plaintiff Peters received notice of the data breach, and a copy of the notice is attached hereto as Exhibit B.

3. Plaintiff GERALDINE PINEDA is, and at all times mentioned herein was, an individual citizen of the State of New Mexico, residing in Los Lunas, New Mexico, and is a patient of Defendant ASSURED. Plaintiff Pineda received notice of the data breach, and a copy of the notice is attached hereto as Exhibit C.

4. Defendant ASSURED is an Arizona domestic limited liability company with its principal place of business and corporate headquarters at 7717 N Hartman Ln, Tucson, AZ 85743. Defendant ASSURED also maintains offices and facilities at 9180 E Desert Cove Ave, Suite 102, Scottsdale, AZ 85260.

II. JURISDICTION AND VENUE

5. This Court has jurisdiction over this action under the Class Action Fairness Act ("CAFA"), 28 U.S.C. § 1332(d). There are at least 100 members in the proposed class, the aggregated claims of the individual Class Members exceed the sum or value of

$5,000,000.00, exclusive of interest and costs, and members of the Proposed Class are citizens of states different from Defendant.

6. This Court has jurisdiction over Defendant, which operates and is headquartered in this District. The computer systems implicated in this Ransomware Attack/Data Breach are likely based in this District. Through its business operations in this District, ASSURED intentionally avails itself of the markets within this District to render the exercise of jurisdiction by this Court just and proper.

7. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(a)(1) because a substantial part of the events and omissions giving rise to this action occurred in this District. Defendant is based in this District, maintains the personally identifiable information ("PII") and protected health information ("PHI") of Plaintiffs and Class members in this District, and has caused harm to Plaintiffs and Class Members through its actions in this District.

III. NATURE OF THE ACTION

8. This class action arises out of the recent targeted ransomware attack at ASSURED's medical facilities that disrupted operations by, among other things, encrypting its medical record system and blocking access to ASSURED's computer systems and data, including the highly sensitive patient medical records of approximately 244,813 patients (the "Ransomware Attack" or "Data Breach"). In addition, the cyber criminals exfiltrated and stole data from ASSURED's systems prior to the deployment of ransomware.

9. As a result of the Ransomware Attack, Plaintiffs and Class Members suffered ascertainable losses in the form of disruption of medical services, out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the attack. In addition, Plaintiffs' and Class Members' sensitive personal information—which was entrusted to ASSURED, its officials and agents—was compromised, unlawfully accessed, exfiltrated, and stolen from Defendant's systems prior to and during the Ransomware Attack. Information compromised in the Ransomware Attack includes

full names, addresses, dates of birth, patient IDs, facility used, treating clinicians' names, medical histories, services performed, assessments of the service performed, and recommendations on future testing, other protected health information as defined by the HIPAA, and additional PII and PHI that Defendant ASSURED collected and maintained (collectively the "Private Information").

10. Plaintiffs bring this class action lawsuit on behalf of those similarly situated to address Defendant's inadequate safeguarding of Class Members' Private Information that it collected and maintained.

11. Defendant maintained the Private Information in a reckless manner. In particular, the Private Information was maintained on Defendant ASSURED's computer network in a condition vulnerable to cyberattacks of the type that cause actual disruption to Plaintiffs' and Class Members' medical care and treatment. As a result of the Ransomware Attack, Plaintiffs' and Class Members' Private Information was encrypted and held hostage by computer hackers for "ransom," and ultimately disclosed to other unknown thieves. Upon information and belief, the mechanism of the ransomware and potential for improper disclosure of Plaintiffs' and Class Members' Private Information was a known risk to Defendant, 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.

12. In addition, ASSURED and its employees failed to properly monitor the computer network and systems that housed the Private Information, did not detect the initial intrusion into its systems that resulted in exfiltration of data, and ultimately only became aware that its systems had been compromised when the ransomware attack was unleashed. Had ASSURED properly monitored its property, it would have discovered the intrusion sooner.

13. Because of the Ransomware Attack, Plaintiffs and Class Members had their medical care and treatment as well as their daily lives disrupted. As a consequence of the ransomware locking down the medical records of Plaintiffs and Class Members, Plaintiffs

and Class Members had to, among other things, forego medical care and treatment or had to seek alternative care and treatment.

14. What's more, aside from having their lives disrupted, Plaintiffs' and Class Members' identities are now at risk because of Defendant's negligent conduct, as the Private Information that Defendant ASSURED collected and maintained is now in the hands of data thieves.

15. Armed with the Private Information accessed and exfiltrated in the initial data breach and subsequent Ransomware Attack, data thieves can commit a variety of crimes including, e.g., 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.

16. As a further result of the Ransomware Attack, 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.

17. Plaintiffs and Class Members may also incur out of pocket costs for, e.g., purchasing credit monitoring services, credit freezes, credit reports, or other protective measures to deter and detect identity theft.

18. By their Complaint, Plaintiffs seek to remedy these harms on behalf of themselves and all similarly situated individuals whose Private Information was accessed, compromised, ransomed, or exfiltrated during the initial data intrusion and subsequent Ransomware Attack.

19. Plaintiffs seek remedies including, but not limited to, compensatory 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.

20. Accordingly, Plaintiffs bring this action against Defendant seeking redress for its unlawful conduct, and asserting claims for: (i) negligence; (ii) negligence *per se*; (iii) breach of express contract; (iv) breach of implied contract; (v) breach of fiduciary duty; (vi) violation of the Arizona Consumer Fraud Act, and; (vii) unjust enrichment

DEFENDANT'S BUSINESS

21. ASSURED bills itself as the leading provider of mobile digital mammography in the United States, operating from more than 60 locations across 16 states. ASSURED maintains permanent imaging center locations in four states – Arizona, New Mexico, Texas, and Washington.

22. ASSURED is currently a subsidiary of Rezolut Medical Imaging, a national emerging platform of diagnostic medical imaging services based in Atlanta, Georgia.

23. ASSURED offers 2D and 3D mammography in both spa style imaging centers and mobile event settings.

24. ASSURED also offers and provides breast and general ultrasound at its imaging centers in Arizona and New Mexico.

25. ASSURED also provides bone densitometry (DEXA) screens for bone mineral density (helping to diagnose osteoporosis and osteopenia) from both its imaging centers and mobile units.

26. ASSURED's specialty vehicle mobile digital mammography services also offer heart health and skin cancer screenings, in addition to the mammography and DEXA services listed above.

27. In the ordinary course of receiving treatment and health care services from Defendant ASSURED, all patients (including the named Plaintiffs here) are required to complete the "Patient Information and Acknowledgement Form," and are required to provide Defendant with sensitive, personal and private information such as:

- Name, address, phone number and email address;

- Date of birth;
- Demographic information;
- Social Security number;
- Information relating to individual medical history (via Defendant's various "Patient History Forms");
- Insurance information and coverage;
- Information concerning an individual's doctor, nurse or other medical providers;
- Photo identification;
- Employer information, and;
- Other information that may be deemed necessary to provide care.

28. Defendant ASSURED also gathers certain medical information about patients and creates records of the care it provides to them.

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

30. Defendant has promulgated and adopted a "Privacy Notice to Patients" ("Privacy Notice") Patient Handout, which memorializes ASSURED's established privacy policy. The Privacy Notice is posted on Defendant's website, and is provided to each patient prior to treatment. *See* Assured Privacy Notices, attached hereto as Exhibit D.

31. Defendant also has promulgated and adopted a "Patient Rights and Responsibilities" ("Patient Rights") Patient Handout, which further memorializes ASSURED's established privacy policy. The Patient Rights are also posted on Defendant's website, and are provided to each patient prior to treatment. *Id.*

32. In the Patient Rights, Defendant states that its patients have "the right to privacy of your medical records. Without your consent, we will not release your medical record unless authorized by law or to those responsible for paying your bill." *Id.*

THE RANSOMWARE ATTACK

33. A ransomware attack is a type of malicious software that blocks access to a computer system or data, usually by encrypting it, until the victim pays a fee to the attacker.[1]

34. Ransomware attacks are often the final piece of a multiphase coordinated cyber-attack. The computer systems of the cyberthieves' target are first infiltrated by malicious software commonly referred to as the "Initial Attack Vector," or "IAV." The IAV creates a means by which other malicious software, such as "Offensive Security Tools" or "OST," further infects the target's computer systems. The OST often contains the capability to exfiltrate data from the target's computer system, and to also erase all records of the malicious activity perpetrated. Once the cyberthieves have plundered the target's system using the IAV and OST, the cybercriminals unleash their ransomware virus, locking down the target's systems for a ransom.

35. On or about May 15, 2020, ASSURED experienced a cybersecurity incident. Upon information and belief, a cyberattack that was launched from the inbox and email of at least one ASSURED employee opened the door for malignant software (aka computer viruses, an IAV, OST, and a ransomware virus variant) to infect ASSURED's computer networks.

36. ASSURED was not aware that its systems were compromised, and between May 15, 2020 and May 17, 2020, the cyberthieves had unfettered access to Defendant's computer systems, and utilized that access to exfiltrate data from ASSURED's systems, including patient data.

[1] https://www.proofpoint.com/us/threat-reference/ransomware.

37. ASSURED did not become aware that its computer systems were compromised and infected until the cyberthieves launched a targeted ransomware attack on May 19, 2020.

38. The attack targeted ASSURED's electronic medical record (EMR) system, which is the information technology ("IT") system that contains considerable amounts of PHI, including the PHI of Plaintiffs and Class Members.

39. Shutting down a medical care provider's EMR system has been called the "nightmare" situation. As a recent new article explains:

> Hospitals depend on digital systems that contain all of their patient information for day-to-day operations to run smoothly. These electronic medical record systems, known as EMRs, can be equated to the "brains of a hospital." Without them, medical care professionals don't have the vital information they need to do the most basic parts of their jobs. If these systems are compromised during an attack, healthcare providers must revert back to pen and paper, diminishing their already limited time spent treating patients.[2]

40. The Ransomware Attack disrupted ASSURED's computer network, leaving patient data stored on ASSURED's network encrypted and inaccessible.

41. The Ransomware Attack shut down ASSURED's EMR and other IT systems for multiple days, as ASSURED worked to restore the encrypted files from backups.

42. As a consequence of the cyber-attack on ASSURED's computer systems, certain affected data was encrypted and locked away by the ransomware. This data included the Protected Health Information, or PHI, of Defendant ASSURED's patients, including Plaintiffs and Class Members, who entrusted Defendant with this highly sensitive and private information.

[2] https://www.healthcarefacilitiestoday.com/posts/What-hospitals-can-learn-from-the-Parkview-Medical-shutdown--24495

43. On or about August 26, 2020, ASSURED notified affected persons and various governmental agencies of the Ransomware Attack/Data Breach. The Notice of Data Incident ("Notice") stated in relevant part the following:

> **Notice of Data Incident**
>
> **What Happened?** On May 19, 2020, Assured learned that its electronic medical records system had become encrypted due to "ransomware" deployed by an unknown actor. Because the impacted systems contained patient information, Assured worked quickly to (1) restore access to the patient information so it could continue to care for patients without disruption and (2) investigate what happened and whether this incident resulted in any unauthorized access to, or theft of, patient information by the unknown actor.
>
> Assured conducted an extensive investigation, with the assistance of third-party computer forensic specialists to determine the nature and scope of the incident. On July 1, 2020, the investigation confirmed Assured systems were accessible by an unknown actor between May 15, 2020 and May 17, 2020, and certain, limited data was exfiltrated from our systems. The investigation was unable to determine the full extent of information that was accessed by the unknown actor. In an abundance of caution, Assured performed a comprehensive review of all information stored in our systems at the time of incident to identify the individuals whose information may have been accessible to the unknown actor. We then worked to determine the identities and contact information for potentially impacted individuals.
>
> **What Information Was Involved**. The following types of patient information were present in the electronic medical records system and therefore potentially accessed and acquired by the unknown actor during this incident during the incident: full name, address, date of birth, patient ID, facility, treating clinician, medical history, service performed, and assessment of the service performed, including any recommendations on future testing. We are unaware that any of the information was misused by the unknown actor and Assured is providing this notice in an abundance of caution.
>
> **What We are Doing**. Assured takes this incident and the security of your personal information seriously. Upon learning of this incident, we immediately took steps to restore our operations and further secure our systems. As part of our ongoing commitment to the privacy of personal information in our care, we are working to review our existing policies and procedures and to implement additional safeguards to further secure the information in our systems. Assured also notified the U.S. Department of Health and Human Services and other government regulators, as required.

> **What Affected Individuals Can Do**. While we are unaware of any misuse of any personal information contained within the impacted system, individuals are encouraged to remain vigilant against incidents of identity theft by reviewing account statements and explanations of benefits for unusual activity and report any suspicious activity immediately to your insurance company, health care provider, or financial institution. Additional detail can be found below, in the *Steps You Can Take to Protect Your Information*.

See Exhibit E, Rezolut Website Notice, https://www.assuredimaging.com/wp-content/uploads/2020/08/Rezolut-HIPAA-Website-Notice.pdf (last accessed on September 10, 2020); *see e.g.* Exhibits A-C. This notice (or one substantially similar) was sent to 244,813 persons, and was reported to the US Department of Health and Human Services on August 27, 2020.

44. Based upon Defendant's admission in its Notice of Data Breach that patient data was exfiltrated, Plaintiffs believe their Private Information was stolen (and subsequently sold) in the Ransomware Attack.

45. Plaintiffs' belief that their Private Information was stolen is buttressed by a recent security advisory blog post from Microsoft that emphasized how healthcare ransomware attackers maintain their presence in breached computer systems (even systems that are rebuilt), and exfiltrate and steal data during these attacks:

> On networks where attackers deployed ransomware, they deliberately maintained their presence on some endpoints, intending to reinitiate malicious activity after ransom is paid or systems are rebuilt. In addition, while only a few of these groups gained notoriety for selling data, almost all of them were observed viewing and exfiltrating data during these attacks, even if they have not advertised or sold yet.[3]

46. Despite learning of the ransomware attack on May 19, 2020, ASSURED did not begin providing notice of the data breach to its patients until August 26, 2020.

[3] https://www.microsoft.com/security/blog/2020/04/28/ransomware-groups-continue-to-target-healthcare-critical-services-heres-how-to-reduce-risk/

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

48. 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.

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

50. Data breaches, including those perpetrated against the healthcare sector of the economy, have become widespread. In 2016, the number of U.S. data breaches surpassed 1,000, a record high and a forty percent increase in the number of data breaches from the previous year. In 2017, a new record high of 1,579 breaches were reported, representing a 44.7 percent increase over 2016. In 2018, there was an extreme jump of 126 percent in the number of consumer records exposed from data breaches. In 2019, there was a 17 percent increase in the number of breaches (1,473) over 2018, with 164,683,455 sensitive records exposed.

51. The number of data breaches in the healthcare sector skyrocketed in 2019, with 525 reported breaches exposing nearly 40 million sensitive records (39,378,157), compared to only 369 breaches that exposed just over 10 million sensitive records (10,632,600) in 2018.

52. Indeed, ransomware attacks, such as the one experienced by Defendant, 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."[4]

53. 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 ASSURED.

DEFENDANT FAILS TO COMPLY WITH FTC GUIDELINES

54. 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.

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

56. 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

[4] 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 (emphasis added).

suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.

57. 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.

58. 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, 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.")

59. Defendant failed to properly implement basic data security practices. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to patient PII and PHI constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

60. Defendant was at all times fully aware of its obligation to protect the PII and PHI of its patients. Defendant was also aware of the significant repercussions that would result from its failure to do so.

DEFENDANT FAILS TO COMPLY WITH INDUSTRY STANDARDS

61. As shown 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.

62. As an article about the recent Microsoft study stated, "All hospitals and healthcare organizations need to defend themselves against ransomware, especially during

this challenging time."[5] Microsoft provided a list of 11 best practices tips for how hospitals should protect themselves against ransomware.

63. 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.

64. A number of industry and national best practices have been published and should be used as a go-to resource when developing an institution's cybersecurity standards. The Center for Internet Security (CIS) released its Critical Security Controls, and all healthcare institutions are strongly advised to follow these actions. The CIS Benchmarks are the overwhelming option of choice for auditors worldwide when advising organizations on the adoption of a secure build standard for any governance and security initiative, including PCI DSS, HIPAA, NIST 800-53, SOX, FISMA, ISO/IEC 27002, Graham Leach Bliley and ITIL.[6]

65. 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.

66. Defendant failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework, NIST Special Publications 800-53, 53A, or 800-171; General Accounting Office (GAO) standards; the Federal Risk and

[5] https://www.techrepublic.com/article/microsoft-to-hospitals-11-tips-on-how-to-combat-ransomware/

[6] https://www.cisecurity.org/cis-benchmarks/cis-benchmarks-faq/

Authorization Management Program (FEDRAMP); and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

67. Defendant failed to meet the following industry standards for cybersecurity: NIST, COBIT 5, PCI DSS, ISO/IEC27001, and ISO/IEC27002.

DEFENDANT'S CONDUCT VIOLATES HIPAA AND EVIDENCES ITS INSUFFICIENT DATA SECURITY

68. As a healthcare service provider, Defendant is bound by the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), which requires subject providers to comply with a series of administrative, physical security, and technical security requirements in order to protect patient information.

69. Defendant ASSURED is a "covered entity" under HIPAA.

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

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

72. 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).

73. Defendant's Ransomware Attack/Data Breach resulted from a combination of insufficiencies that demonstrate it failed to comply with safeguards mandated by HIPAA regulations.

DEFENDANT'S BREACH

74. Defendant breached its obligations to Plaintiffs and Class Members and/or was otherwise negligent and reckless because it failed to properly maintain and safeguard the ASSURED computer systems and data. 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 patients' Private Information;

c. Failing to properly monitor its own data security systems for existing intrusions, brute-force attempts, and clearing of event logs;

d. Failing to apply all available security updates;

e. Failing to install the latest software patches, update its firewalls, check user account privileges, or ensure proper security practices;

f. Failing to practice the principle of least-privilege and maintain credential hygiene

g. Failing to avoid the use of domain-wide, admin-level service accounts;

h. Failing to employ or enforce the use of strong randomized, just-in-time local administrator passwords;

i. Failing to properly train and supervise employees in the proper handling of inbound emails;

j. 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);

k. 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);

l. 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);

m. 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);

n. 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);

o. 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);

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

q. 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

r. 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 definition of encryption).

75. As the result of computer systems in dire need of security upgrading, inadequate procedures for handling emails containing ransomware or other malignant computer code, and inadequately trained employees who opened files containing the ransomware virus, Defendant ASSURED negligently and unlawfully failed to safeguard Plaintiffs' and Class Members' Private Information.

76. Accordingly, as outlined below, Plaintiffs' and Class Members' medical care and daily lives were severely disrupted. What's more, they now face an increased risk of fraud and identity theft.

RANSOMWARE ATTACKS AND DATA BREACHES CAUSE DISRUPTION AND PUT CONSUMERS AT AN INCREASED RISK OF FRAUD AND IDENTIFY THEFT

77. Ransomware attacks at medical facilities such as Defendant ASSURED's are especially problematic because of the disruption they cause to the medical treatment and overall daily lives of patients affected by the attack.

78. For instance, loss of access to patient histories, charts, images and other information forces providers to limit or cancel patient treatment because of the disruption of service.

79. This leads to a deterioration in the quality of overall care patients receive at facilities affected by ransomware attacks and related data breaches.

80. Researchers have found that at medical facilities that experienced a data security incident, the death rate among patients increased in the months and years after the attack.[7]

81. Researchers have further found that at medical facilities that experienced a data security incident, the incident was associated with deterioration in patient outcomes, generally.[8]

---

[7] *See* https://www.pbs.org/newshour/science/ransomware-and-other-data-breaches-linked-to-uptick-in-fatal-heart-attacks.

[8] *See* https://onlinelibrary.wiley.com/doi/full/10.1111/1475-6773.13203.

82. Similarly, ransomware attacks and related data security incidents inconvenience patients. Inconveniences patients encounter as a result of such incidents include, but are not limited to, the following:

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.[9]

83. Ransomware attacks such as this one, where ASSURED confirms that data was exfiltrated, also constitute data breaches in the traditional sense. For example, in a recent ransomware attack on the Florida city of Pensacola, and while the City was still recovering from the ransomware attack, hackers released 2GB of data files from the total 32GB of data that they claimed was stolen prior to encrypting the City's network with the maze ransomware. In the statement given to a news outlet, the hackers said, "***This is the fault of mass media who writes that we don't exfiltrate data***…."[10]

84. Also, in a ransomware advisory, the Department of Health and Human Services informed entities covered by HIPAA that "when electronic protected health information (ePHI) is encrypted as the result of a ransomware attack, a breach has occurred because the ePHI encrypted by the ransomware was acquired (i.e., unauthorized individuals have taken possession or control of the information)."[11]

---

[9] *See, e.g.*, https://nakedsecurity.sophos.com/2019/10/03/ransomware-attacks-paralyze-and-sometimes-crush-hospitals/; https://healthitsecurity.com/news/data-breaches-will-cost-healthcare-4b-in-2019-threats-outpace-tech.

[10] https://www.cisomag.com/pensacola-ransomware-hackers-release-2gb-data-as-a-proof/

[11] *See* https://www.hhs.gov/sites/default/files/RansomwareFactSheet.pdf.

85. Ransomware attacks are also 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." See 45 C.F.R. 164.40[12]

86. Other security experts agree that when ransomware attack occurs, a data breach does as well, because such an attack represents a loss of control of the data within a network.[13]

87. Ransomware attacks are also Security Incidents under HIPAA because they impair both the integrity (data is not interpretable) and availability (data is not accessible) of patient health information:

> The presence of ransomware (or any malware) on a covered entity's or business associate's computer systems is a security incident under the HIPAA Security Rule. A security incident is defined as the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system. See the definition of security incident at 45 C.F.R. 164.304. Once the ransomware is detected, the covered entity or business associate must initiate its security incident and response and reporting procedures. See 45 C.F.R.164.308(a)(6).[14]

88. Data breaches represent yet another problem for patients who have already experienced inconvenience and disruption associated with a ransomware attack.

89. The United States Government Accountability Office released a report in 2007 regarding data breaches ("GAO Report") in which it noted that victims of identity

---

[12] *Id.*

[13] *See e.g.*, https://www.csoonline.com/article/3385520/how-hackers-use-ransomware-to-hide-data-breaches-and-other-attacks.html; https://www.varonis.com/blog/is-a-ransomware-attack-a-data-breach/; https://digitalguardian.com/blog/ransomware-infection-always-data-breach-yes.

[14] See https://www.hhs.gov/sites/default/files/RansomwareFactSheet.pdf

theft will face "substantial costs and time to repair the damage to their good name and credit record."[15]

90. 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.[16]

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

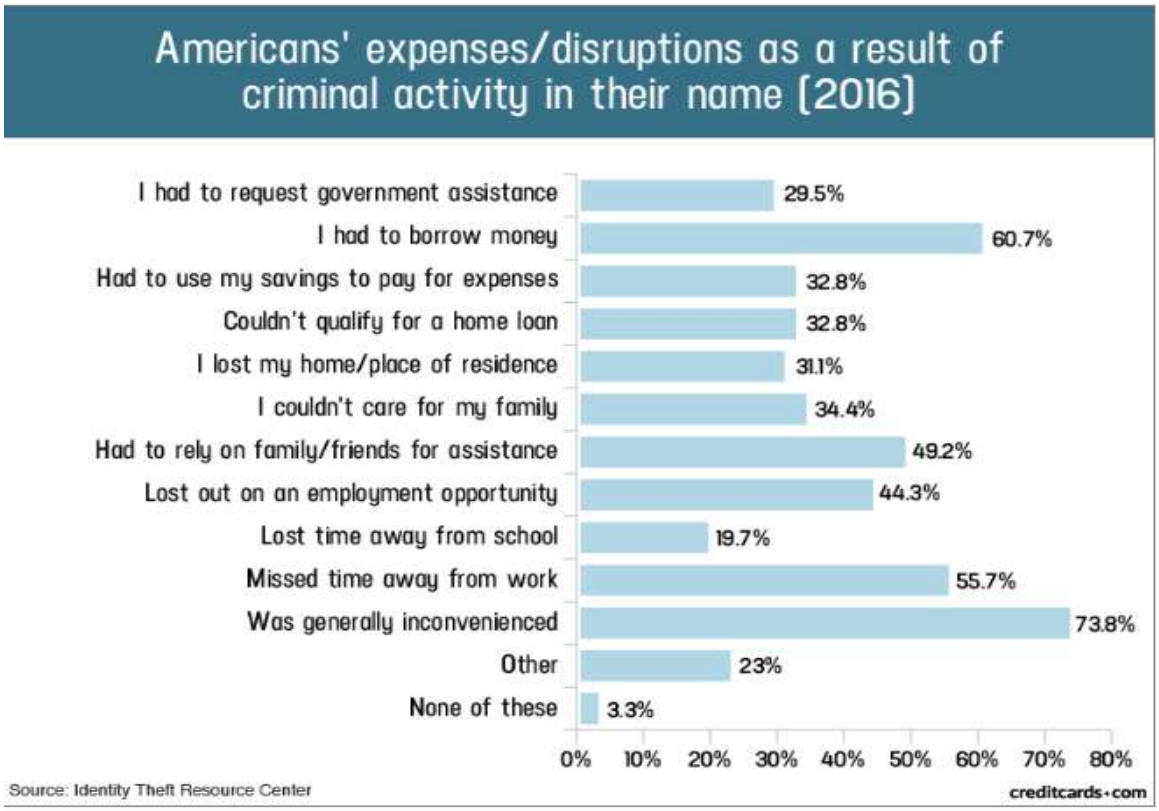
92. Identity thieves can also use Social Security numbers to obtain a driver's license or official identification card in the victim's name but with the thief's picture; use the victim's name and Social Security number to obtain government benefits; or file a fraudulent tax return using the victim's information. 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. A study by Identity Theft Resource Center shows the multitude of harms caused by fraudulent use of personal and financial information:[17]

---

[15] *See* "Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown," p. 2, U.S. Government Accountability Office, June 2007, https://www.gao.gov/new.items/d07737.pdf (last visited Apr. 12, 2019) ("GAO Report").

[16] *See* https://www.identitytheft.gov/Steps (last visited April 12, 2019).

[17] "Credit Card and ID Theft Statistics" by Jason Steele, 10/24/2017, at: https://www.creditcards.com/credit-card-news/credit-card-security-id-theft-fraud-statistics-1276.php (last visited June 20, 2019).



93. What's more, theft of Private Information is also gravely serious. PII/PHI is a valuable property right.[18] Its value is axiomatic, considering the value of Big Data in corporate America and 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.

94. 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, insurance and payment records, and credit report may be affected."[19] Drug

[18] *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).

[19] *See* Federal Trade Commission, Medical Identity Theft, http://www.consumer.ftc.gov/articles/0171-medical-identity-theft (last visited March 27, 2020).

manufacturers, medical device manufacturers, pharmacies, hospitals and other healthcare service providers often purchase PII/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.

95. It must also be noted there may be a substantial time lag – measured in years -- between when harm occurs versus when it is discovered, and also between when Private Information and/or financial information is stolen and when it is used. 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 p. 29.

96. Private Information 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.

97. 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.

98. Medical information is especially valuable to identity thieves. 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. That pales in

comparison with the asking price for medical data, which was selling for $50 and up.[20]

99. Because of its value, the medical industry has experienced disproportionally higher numbers of data theft events than other industries. Defendant therefore knew or should have known this and strengthened its data systems accordingly. Defendant was put on notice of the substantial and foreseeable risk of harm from a data breach, yet it failed to properly prepare for that risk.

PLAINTIFFS' AND CLASS MEMBERS' DAMAGES

100. To date, Defendant has done absolutely nothing to provide Plaintiffs and Class Members with relief for the damages they have suffered as a result of the Ransomware Attack. Nor has Defendant offered any protection against the imminent, likely, and probable effects that will result from Plaintiffs' and Class Members' Private Information being stolen in connection with the attack.

101. Plaintiffs and Class Members have been damaged by the compromise of their Private Information in the Ransomware Attack.

102. As a direct and proximate result of Defendant's conduct, Plaintiffs and Class Members had their medical care and treatment disrupted and compromised.

103. 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.

104. 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.

105. 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 target such schemes more effectively to Plaintiffs and Class Members.

---

[20] https://nakedsecurity.sophos.com/2019/10/03/ransomware-attacks-paralyze-and-sometimes-crush-hospitals/#content.

106. Plaintiffs and Class Members may also incur out-of-pocket costs for protective measures such as credit monitoring fees, credit report fees, credit freeze fees, and similar costs directly or indirectly related to the Ransomware Attack.

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

108. Class Members were also damaged via benefit-of-the-bargain damages, in that they 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 Defendant ASSURED's computer property and Plaintiffs' and Class Members' Private Information. Thus, Plaintiffs and the Class Members did not get what they paid for.

109. Plaintiffs and Class Members have spent and will continue to spend significant amounts of time to monitor their financial and medical accounts and records for misuse.

110. Plaintiffs and Class Members have suffered or will suffer actual injury as a direct result of the Ransomware Attack. In addition to the loss of use of and access to their medical records and costs associated with the inability to access their medical records (including actual disruption of medical care and treatment), 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 Ransomware Attack relating to:

a. Finding alternative medical care and treatment;
b. Delaying or foregoing medical care and treatment;
c. Undergoing medical care and treatment without medical providers having access to a complete medical history and records;
d. Having to retrace or recreate their medical history;
e. Finding fraudulent charges;

f. Canceling and reissuing credit and debit cards;

g. Purchasing credit monitoring and identity theft prevention;

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

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

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

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

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

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

n. 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

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

111. 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 personal and financial information is not accessible online and that access to such data is password-protected.

112. 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.

113. 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.

IV. CLASS ACTION ALLEGATIONS

114. Plaintiffs bring this action on behalf of themselves and on behalf of all other persons similarly situated ("the Class").

115. Plaintiffs propose the following Class definition, subject to amendment as appropriate:

> All persons whose PII and PHI was compromised as a result of the Ransomware Attack that ASSURED IMAGING discovered on or about May 19, 2020.

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.

116. Plaintiffs hereby reserve the right to amend or modify the class definition with greater specificity or division after having had an opportunity to conduct discovery. The proposed Class meets the criteria for certification under Rule 23(a), (b)(2), (b)(3) and (c)(4).

117. 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 Plaintiffs at this time, based on information and belief, the Class consists of 244,813 patients of Defendant ASSURED whose data was compromised in the Ransomware Attack.

118. 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 Ransomware Attack;

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

d) Whether Defendant's data security systems prior to and during the Ransomware Attack 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;

g) Whether computer hackers obtained Class Members' Private Information in the Ransomware attack;

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

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

j) Whether Defendant owed a duty to provide Plaintiffs and Class Members notice of this data breach, and whether Defendant breached that duty;

k) Whether Defendant's conduct was negligent;

l) Whether Defendant's conduct was *per se* negligent;

m) Whether Defendant was unjustly enriched;

n) Whether Defendant violated the Arizona Consumer Fraud Act, and;

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

119. 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 Ransomware Attack.

120. 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.

121. Predominance. Defendant has 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 systems 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.

122. 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 claim 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.

123. 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.

124. Likewise, particular issues under Rule 23(c)(4) 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:

a. Whether Defendant failed to timely notify the public of the Data Breach;

b. Whether Defendant owed a legal duty to Plaintiffs and the Class to exercise due care in collecting, storing, and safeguarding their PII and PHI;

c. Whether Defendant's security measures to protect its data systems were reasonable in light of best practices recommended by data security experts;

d. Whether Defendant's failure to institute adequate protective security measures amounted to negligence;

e. Whether Defendant failed to take commercially reasonable steps to safeguard consumer PII and PHI; and

f. Whether adherence to FTC data security recommendations, and measures recommended by data security experts would have reasonably prevented the data breach.

125. Finally, all members of the proposed Class are readily ascertainable. Defendant has access to Class Members' names and addresses affected by the Data Breach. Class Members have already been preliminarily identified and sent notice of the Data Breach by Defendant ASSURED.

/ / /

/ /

V. CAUSES OF ACTION

FIRST COUNT
Negligence
(On Behalf of Plaintiffs and All Class Members)

126. Plaintiffs re-allege and incorporate by reference Paragraphs 1 through 125 above as if fully set forth herein

127. Defendant required Plaintiffs and Class Members to submit non-public personal information in order to obtain medical services.

128. By collecting and storing this data in its computer property, and sharing it and using it for commercial gain, Defendant had 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 theft. Defendant's duty included a responsibility to implement processes by which it 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.

129. 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.

130. Defendant's duty of care to use reasonable security measures arose as a result of the special relationship that existed between Defendant and its client patients, which is recognized by laws and regulations including but not limited to HIPAA, as well as common law. Defendant was in a position to ensure that its systems were sufficient to protect against the foreseeable risk of harm to Class Members from a data breach.

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

132. 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.

133. 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.

134. 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 its networks and systems;
c. Failure to periodically ensure that its email system had plans in place to maintain reasonable data security safeguards;
d. Allowing unauthorized access to Class Members' Private Information;
e. Failing to detect in a timely manner that Class Members' Private Information had been compromised; and
f. Failing to timely notify Class Members about the Ransomware Attack so that they could take appropriate steps to mitigate the potential for identity theft and other damages.

135. It was foreseeable that Defendant's failure to use reasonable measures to protect Class Members' Private Information would result in injury to Class Members. Further, the breach of security was reasonably foreseeable given the known high frequency of cyberattacks and data breaches in the medical industry.

136. 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.

137. Plaintiffs and Class Members are entitled to compensatory and consequential damages suffered as a result of the Ransomware Attack.

138. Plaintiffs and Class Members are also entitled to injunctive relief requiring Defendant to (i) strengthen its 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
Negligence *Per Se*
(On Behalf of Plaintiffs and All Class Members)

139. Plaintiffs re-allege and incorporate by reference Paragraphs 1 through 125 above as if fully set forth herein.

140. Pursuant to Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, Defendant had a duty to provide fair and adequate computer systems and data security practices to safeguard Plaintiffs' and Class Members' Private Information.

141. Plaintiffs and Class Members are within the class of persons that the FTCA was intended to protect.

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

143. Pursuant to HIPAA, 42 U.S.C. § 1302d, *et seq.*, Defendant had a duty to implement reasonable safeguards to protect Plaintiffs' and Class Members' Private Information.

144. Pursuant to HIPAA, Defendant 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." *See* definition of encryption at 45 C.F.R. § 164.304.

145. Plaintiffs and Class Members are within the class of persons that the HIPAA was intended to protect.

146. The harm that occurred as a result of the Data Breach is the type of harm that HIPAA was intended to guard against. The Federal Health and Human Services' Office for Civil Rights ("OCR") has pursued enforcement actions against businesses, which, as a result of their failure to employ reasonable data security measures relating to protected health information, caused the same harm as that suffered by Plaintiffs and the Class.

147. Defendant breached its duties to Plaintiffs and Class Members under the Federal Trade Commission Act and HIPAA by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiffs' and Class Members' Private Information.

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

149. But for Defendant's wrongful and negligent breach of its duties owed to Plaintiffs and Class Members, Plaintiffs and Class Members would not have been injured.

150. The injury and harm suffered by Plaintiffs and Class Members was the reasonably foreseeable result of Defendant's breach of its duties. Defendant knew or should have known that it was failing to meet its duties, and that Defendant's breach would

cause Plaintiffs and Class Members to experience the foreseeable harms associated with the exposure of their Private Information.

151. As a direct and proximate result of Defendant'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.

THIRD COUNT
Breach of Express Contract
(On Behalf of Plaintiffs and All Class Members)

152. Plaintiffs re-allege and incorporate by reference Paragraphs 1 through 125 above as if fully set forth herein.

153. Plaintiffs and Members of the Class allege that they entered into valid and enforceable express contracts with Defendant for the provision of medical and health care services.

154. Specifically, Plaintiffs entered into a valid and enforceable express contract with Defendant when they first went for mammography services and other medical care and treatment at one of Defendant's facilities.

155. The valid and enforceable express contracts to provide medical and health care services that Plaintiffs and Class Members entered into with Defendant include Defendant's promise to protect nonpublic Private Information given to Defendant or that Defendant gathers on its own from disclosure.

156. 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' PII/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, and to turn over their Private Information.

157. Both the provision of medical services healthcare and the protection of Plaintiffs and Class Members' Private Information were material aspects of these express contracts.

158. The express contracts for the provision of medical services – contracts that include the contractual obligations to maintain the privacy of Plaintiffs' and Class Members' Private Information—are formed and embodied in multiple documents, including (among other documents) Defendant's Privacy Notice and Patient's Rights document.

159. At all relevant times, Defendant expressly represented in its Patients' Rights document that patients had "the right to privacy of your medical records," and that "[wi]thout your consent, we will not release your medical record unless authorized by law or to those responsible for paying your bill."

160. Defendant's express representations, including, but not limited to the express representations found in its Patients' Rights document, formed and embodied an express contractual obligation requiring Defendant to implement data security adequate to safeguard and protect the privacy of Plaintiffs and Class Members' Private Information.

161. Consumers of healthcare value their privacy, the privacy of their dependents, and the ability to keep their Private Information associated with obtaining healthcare private. To customers such as Plaintiffs and Class Members, healthcare that does not adhere to industry standard data security protocols to protect Private Information 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 these contracts with Defendant and/or its affiliated healthcare providers as a direct or third-party beneficiary without an understanding that their Private Information would be safeguarded and protected.

162. A meeting of the minds occurred, as Plaintiffs and Members of the Class agreed to and did provide their Private Information to Defendant and/or its affiliated healthcare providers, and paid for the provided healthcare in exchange for, amongst other

things, both the provision of healthcare and medical services and the protection of their Private Information.

163. Plaintiffs and Class Members performed their obligations under the contract when they paid for their health care services and provided their Private Information.

164. Defendant materially breached its contractual obligation to protect the nonpublic Private Information Defendant gathered when the information was accessed and exfiltrated by unauthorized personnel as part of the Ransomware Attack.

165. Defendant materially breached the terms of these express contracts, including, but not limited to, the terms stated in the relevant Notice of Privacy Practices and Patients' Rights documents. *See* Exhibit D. Defendant did not maintain the privacy of Plaintiffs' and Class Members' Private Information as evidenced by its notifications of the Data Breach to Plaintiffs and approximately 244,813 Class Members. Specifically, Defendant did not comply with industry standards, standards of conduct embodied in statutes like HIPAA and Section 5 of the FTCA, or otherwise protect Plaintiffs' and the Class Members' Private Information, as set forth above.

166. The Ransomware Attack was a reasonably foreseeable consequence of Defendant's actions in breach of these contracts.

167. As a result of Defendant'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.

168. Had Defendant 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 Defendant and/or its affiliated healthcare providers.

169. As a direct and proximate result of the Ransomware Attack/Data Breach, Plaintiffs and Class Members have been harmed and have suffered, and will continue to suffer, actual damages and injuries, including without limitation the release and disclosure of their Private Information, the loss of control of their Private Information, 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 Defendant.

170. Plaintiffs and Class Members are entitled to compensatory and consequential damages suffered as a result of the Ransomware Attack/Data Breach.

FOURTH COUNT
Breach of Implied Contract
(On Behalf of Plaintiffs and All Class Members)

171. Plaintiffs re-allege and incorporate by reference Paragraphs 1 through 125 above as if fully set forth herein.

172. Through their course of conduct, Defendant, Plaintiffs, and Class Members entered into implied contracts for the provision of medical care and treatment, as well as implied contracts for the Defendant to implement data security adequate to safeguard and protect the privacy of Plaintiffs and Class Members' Private Information.

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

174. Defendant solicited and invited Class Members to provide their Private Information as part of Defendant's regular business practices. Plaintiffs and Class Members accepted Defendant's offers and provided their Private Information to Defendant.

175. 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.

176. 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.

177. 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.

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

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

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

181. Plaintiffs and Class Members are entitled to compensatory and consequential damages suffered as a result of the Ransomware Attack.

182. 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 All Class Members)

183. Plaintiffs re-allege and incorporate by reference Paragraphs 1 through 125 above as if fully set forth herein.

184. In providing their Private Information to Defendant, Plaintiffs and Class Members justifiably placed special confidence in Defendant to act in good faith and with due regard to interests of Plaintiffs and Class Members to safeguard and keep confidential that Private Information.

185. ASSURED accepted the special confidence placed in it by Plaintiffs and Class Members, as evidence by the statement in its Privacy Notice, that it is "committed to preserving the confidentiality of your health information created or maintained at our medical center," and there was an understanding between the parties that ASSURED would act for the benefit of Plaintiffs and Class Members in preserving the confidentiality of the Private Information.

186. 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 patients, including Plaintiffs and Class Members, for the safeguarding of Plaintiffs' and Class Members' Private Information.

187. Defendant has a fiduciary duty to act for the benefit of Plaintiffs and Class Members upon matters within the scope of its patients' relationship, in particular, to keep secure the Private Information of its patients.

188. Defendant breached its fiduciary duties to Plaintiffs and Class Members by failing to diligently discovery, investigate, and give notice of the Ransomware Attack in a reasonable and practicable period of time.

189. 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.

190. 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 Ransomware Attack.

191. 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).

192. 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).

193. 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).

194. 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).

195. 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).

196. 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).

197. 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).

198. 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.

199. 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).

200. 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).

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

202. As a direct and proximate result of Defendant's breaches 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 Ransomware Attack, 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 Ransomware Attack for the remainder of the lives of Plaintiffs and Class Members; and (vii) the diminished value of Defendant's services they received.

203. As a direct and proximate result of Defendant's breaches of 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
ARIZONA CONSUMER FRAUD ACT ("ACFA")
Ariz. Rev. Stat. §§ 44-1521, et seq.
(On Behalf of Plaintiffs and the Class)

204. Plaintiffs restate and reallege paragraphs 1 through 125 as if fully set forth herein.

205. The ACFA provides in pertinent part: "The act, use or employment by any person of any deception, deceptive or unfair act or practice, fraud, false pretense, false promise, misrepresentation, or concealment, suppression or omission of any material fact with intent that others rely on such concealment, suppression or omission, in connection with the sale or advertisement of any merchandise whether or not any person has in face been misled, deceived or damaged thereby, is declared to be an unlawful practice." Ariz. Rev. Stat. § 44-1522.

206. Plaintiffs and Class Members are "persons" as defined by Ariz. Rev. Stat. § 44-1521(6).

207. Defendant provides "services" as that term is included in the definition of "merchandise" under Ariz. Rev. Stat. § 44-1521(5), and Defendant is engaged in the "sale" of "merchandise" as defined by Ariz. Rev. Stat. § 44-1521(7).

208. Defendant engaged in deceptive and unfair acts and practices, misrepresentation, and the concealment, suppression and omission of material facts in connection with the sale and advertisement of "merchandise" (as defined in the ACFA) in violation of the ACFA, including but not limited to the following:

a. Failing to maintain sufficient security to keep Plaintiffs' and Class Members' confidential medical, financial and personal data from being hacked and stolen;

b. Failing to disclose the Data Breach to Class Members in a timely and accurate manner, in violation of Ariz. Rev. Stat. § 18-552(B);

c. Misrepresenting material facts, pertaining to the sale of health benefit services by representing that it would maintain adequate data privacy and security practices and procedures to safeguard Class Members' PHI and PII from unauthorized disclosure, release, data breaches, and theft;

d. Misrepresenting material facts, in connection with the sale of health benefit services by representing that it did and would comply with the requirements of relevant federal and state laws pertaining to the privacy and security of Class Members' PHI and PII;

e. Omitting, suppressing, and concealing the material fact of the inadequacy of the data privacy and security protections for Class Members' PHI and PII;

f. Engaging in unfair, unlawful, and deceptive acts and practices with respect to the sale of health benefit services by failing to maintain the privacy and security of Class Members' PHI and PII, in violation of duties imposed by and public policies reflected in applicable federal and state laws, resulting in the Data Breach. These unfair, unlawful, and deceptive acts and practices violated duties imposed by laws, including HIPAA and Section 5 of the FTC Act;

g. Engaging in unlawful, unfair, and deceptive acts and practices with respect to the sale of health benefit services by failing to disclose the Data Breach to Class Members in a timely and accurate manner;

h. Engaging in unlawful, unfair, and deceptive acts and practices with respect to the sale of health benefit services by failing to take proper action following the Data Breach to enact adequate privacy and

security measures and protect Class Members' PHI and PII from further unauthorized disclosure, release, data breaches, and theft.

209. The above unlawful, unfair, and deceptive acts and practices by ASSURED were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury to Plaintiffs and Class Members that they could not reasonably avoid; this substantial injury outweighed any benefits to consumers or to competition.

210. Defendant knew or should have known that its computer systems and data security practices were inadequate to safeguard Class Members' PHI and PII and that risk of a data breach or theft was high. ASSURED's actions in engaging in the above-named deceptive acts and practices were negligent, knowing and willful, and/or wanton and reckless with respect to the rights of Members of the Class.

211. As a direct and proximate result of Defendant's deceptive acts and practices, the Class Members suffered an ascertainable loss of money or property, real or personal, as described above, including the loss of their legally protected interest in the confidentiality and privacy of their PHI and PII.

212. Plaintiffs and Class Members seek relief under the ACFA including, but not limited to, injunctive relief, actual damages, treble damages for each willful or knowing violation, and attorneys' fees and costs.

SEVENTH COUNT
Unjust Enrichment
(On Behalf of Plaintiffs and All Class Members)

213. Plaintiffs restate and reallege paragraphs 1 through 125 above as if fully set forth herein, and plead this count in the alternative to the breach of contract counts above.

214. Plaintiffs and Class Members conferred a monetary benefit on Defendant. Specifically, Defendant enriched itself by saving the costs it reasonably should have expended on data security measures to secure Plaintiffs' and Class Members' Personal Information. Instead of providing a reasonable level of security that would have prevented the Ransomware Attack, Defendant instead calculated to increase its own profits 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' decision to prioritize its own profits over 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 PII 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, they would not have agreed to provide their PII to Defendant ASSURED.

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 fails to undertake appropriate and adequate measures to protect PII and PHI 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 PII and PHI compromised as a result of the Data Breach for the remainder of the lives of Plaintiffs 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 it 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.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs pray for judgment as follows:

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

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 Ransomware Attack;

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: September 11, 2020

Respectfully submitted,

ZIMMERMAN REED LLP

By: s/ Hart L. Robinovitch
Hart L. Robinovitch (AZ SBN 020910)
14646 North Kierland Blvd., Suite 145
Scottsdale, AZ 85254
Telephone: (480) 348-6400
Facsimile: (480) 348-6415
Email: hart.robinovitch@zimmreed.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
Telephone: (202) 640-1160
Facsimile: (202) 429-2294
Email: gmason@masonllp.com
Email:dlietz@masonllp.com

MASON LIETZ & KLINGER LLP
Gary M. Klinger (*pro hac vice forthcoming*)
227 W. Monroe Street, Suite 2100
Chicago, IL 60630
Telephone: (202) 640-1160
Facsimile: (202) 429-2294
Email: gklinger@masonllp.com

Attorneys for Plaintiffs and the Proposed Class

UNITED STATES DISTRICT COURT
DISTRICT OF ARIZONA

Civil Cover Sheet

This automated JS-44 conforms generally to the manual JS-44 approved by the Judicial Conference of the United States in September 1974. The data is required for the use of the Clerk of Court for the purpose of initiating the civil docket sheet. The information contained herein neither replaces nor supplements the filing and service of pleadings or other papers as required by law. This form is authorized for use only in the District of Arizona.

The completed cover sheet must be printed directly to PDF and filed as an attachment to the Complaint or Notice of Removal.

Plaintiff(s): **Angela T. Travis ; Kerri G. Peters ; Geraldine Pineda**

County of Residence: Outside the State of Arizona

County Where Claim For Relief Arose: Pima

Plaintiff's Atty(s):

Hart L. Robinovitch
Zimmerman Reed LLP
14646 N Kierland Blvd, Suite 145
Scottsdale, Arizona 85254
4803486400

Defendant(s): **Assured Imaging, LLC**

County of Residence: Pima

Defendant's Atty(s):

II. Basis of Jurisdiction: **4. Diversity (complete item III)**

III. Citizenship of Principal Parties **(Diversity Cases Only)**

Plaintiff:- **2 Citizen of Another State**
Defendant:- **1 Citizen of This State**

IV. Origin : **1. Original Proceeding**

V. Nature of Suit: **370 Other Fraud**

VI.Cause of Action: **Class Action Fairness Act ("CAFA"), 28 U.S.C § 1332(d).**

VII. Requested in Complaint

Class Action: **Yes**
Dollar Demand: + **$5,000,000**
Jury Demand: **Yes**

VIII. This case **is not related** to another case.

Signature: s/ Hart L. Robinovitch

Date: 9/11/2020

If any of this information is incorrect, please go back to the Civil Cover Sheet Input form using the *Back* button in your browser and change it. Once correct, save this form as a PDF and include it as an attachment to your case opening documents.

Revised: 01/2014

EXHIBIT A

assuredimaging
women's wellness

August 31, 2020

Angela T. Travis
[redacted]
Burien, WA [redacted]
P12T535

Re: Notice of Data Breach

Dear Angela T. Travis:

Assured Imaging ("Assured") is writing to inform you of a recent event that may impact the security of some of your information. Although we are unaware of any actual misuse of your information, we are providing you with information about the event, our response, and steps you may take to better protect against the possibility of identity theft and fraud, should you feel it is necessary to do so.

What Happened? On May 19, 2020, Assured learned that its electronic medical records system had become encrypted due to "ransomware" deployed by an unknown actor. Because the impacted systems contained patient information, Assured worked quickly to (1) restore access to the patient information so it could continue to care for patients without disruption and (2) investigate what happened and whether this incident resulted in any unauthorized access to, or theft of, patient information by the unknown actor.

Assured conducted an extensive investigation, with the assistance of third-party computer forensic specialists to determine the nature and scope of the incident. On July 1, 2020, the investigation confirmed Assured systems were accessible by an unknown actor between May 15, 2020 and May 17, 2020, and certain, limited data was exfiltrated from our systems. The investigation was unable to determine the full extent of information that was accessed by the unknown actor. In an abundance of caution, we performed a comprehensive review of all information stored in our systems at the time of incident to identify the individuals whose information may have been accessible to the unknown actor. We then worked to determine the identities and contact information for potentially impacted individuals.

What Information Was Involved. We determined the following types of information relating to you were present in the electronic medical records system and therefore potentially accessed by the unknown actor during this incident: full name, address, date of birth, patient ID, facility, treating clinician, medical history, service performed, and assessment of the service performed, including any recommendations on future testing. We are unaware that any of this information was misused by the unknown actor and Assured is providing this notice in an abundance of caution.

What We Are Doing. We take this incident and the security of your personal information seriously. Upon learning of this incident, we immediately took steps to restore our operations and further secure our systems. As part of our ongoing commitment to the privacy of personal information in our care, we are working to review our existing policies and procedures and to implement additional safeguards to further secure the information in our systems. Assured also notified the U.S. Department of Health and Human Services and other government regulators, as required.

What You Can Do. You can find out more about how to protect against potential identity theft and fraud in the enclosed *Steps You Can Take to Help Protect Your Information.* We encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements and explanations of benefits, and to monitor your credit reports for suspicious activity.

For More Information. If you have additional questions, please call our dedicated assistance line at 1-866-938-0442, Monday through Friday (excluding U.S. holidays), during the hours of 8:00 a.m. to 5:00 p.m., Pacific Time (excluding U.S. holidays). You may also write to Assured at 7717 N. Hartman Lane, Tucson, AZ 85743.

We sincerely regret any inconvenience or concern this incident may cause.

Sincerely,

Kyle J. Dulock
Chief Privacy Officer
Assured Imaging

EXHIBIT B

assuredimaging
women's wellness

August 31, 2020

Kerri G. Peters
[redacted]
Los Lunas, NM [redacted] P4T102

Re: Notice of Data Breach

Dear Kerri G. Peters:

Assured Imaging ("Assured") is writing to inform you of a recent event that may impact the security of some of your information. Although we are unaware of any actual misuse of your information, we are providing you with information about the event, our response, and steps you may take to better protect against the possibility of identity theft and fraud, should you feel it is necessary to do so.

What Happened? On May 19, 2020, Assured learned that its electronic medical records system had become encrypted due to "ransomware" deployed by an unknown actor. Because the impacted systems contained patient information, Assured worked quickly to (1) restore access to the patient information so it could continue to care for patients without disruption and (2) investigate what happened and whether this incident resulted in any unauthorized access to, or theft of, patient information by the unknown actor.

Assured conducted an extensive investigation, with the assistance of third-party computer forensic specialists to determine the nature and scope of the incident. On July 1, 2020, the investigation confirmed Assured systems were accessible by an unknown actor between May 15, 2020 and May 17, 2020, and certain, limited data was exfiltrated from our systems. The investigation was unable to determine the full extent of information that was accessed by the unknown actor. In an abundance of caution, we performed a comprehensive review of all information stored in our systems at the time of incident to identify the individuals whose information may have been accessible to the unknown actor. We then worked to determine the identities and contact information for potentially impacted individuals.

What Information Was Involved. We determined the following types of information relating to you were present in the electronic medical records system and therefore potentially accessed by the unknown actor during this incident: full name, address, date of birth, patient ID, facility, treating clinician, medical history, service performed, and assessment of the service performed, including any recommendations on future testing. We are unaware that any of this information was misused by the unknown actor and Assured is providing this notice in an abundance of caution.

What We Are Doing. We take this incident and the security of your personal information seriously. Upon learning of this incident, we immediately took steps to restore our operations and further secure our systems. As part of our ongoing commitment to the privacy of personal information in our care, we are working to review our existing policies and procedures and to implement additional safeguards to further secure the information in our systems. Assured also notified the U.S. Department of Health and Human Services and other government regulators, as required.

STEPS YOU CAN TAKE TO HELP PROTECT YOUR INFORMATION

Monitor Your Accounts

We encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements, and to monitor your credit reports for suspicious activity. Under U.S. law you are entitled to one free credit report annually from each of the three major credit reporting bureaus. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also contact the three major credit bureaus directly to request a free copy of your credit report.

You have the right to place a "security freeze" on your credit report, which will prohibit a consumer reporting agency from releasing information in your credit report without your express authorization. The security freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a security freeze to take control over who gets access to the personal and financial information in your credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, you cannot be charged to place or lift a security freeze on your credit report. Should you wish to place a security freeze, please contact the major consumer reporting agencies listed below:

Experian
P.O. Box 9554
Allen, TX 75013
1-888-397-3742
www.experian.com/freeze/center.html

TransUnion
P.O. Box 160
Woodlyn, PA 19094
1-888-909-8872
www.transunion.com/credit-freeze

Equifax
P.O. Box 105788
Atlanta, GA 30348-5788
1-800-685-1111
www.equifax.com/personal/credit-report-services

In order to request a security freeze, you will need to provide the following information:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. If you have moved in the past five (5) years, provide the addresses where you have lived over the prior five years;
5. Proof of current address, such as a current utility bill or telephone bill;
6. A legible photocopy of a government-issued identification card (state driver's license or ID card, military identification, etc.);
7. If you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft.

As an alternative to a security freeze, you have the right to place an initial or extended "fraud alert" on your file at no cost. An initial fraud alert is a 1-year alert that is placed on a consumer's credit file. Upon seeing a fraud alert display on a consumer's credit file, a business is required to take steps to verify the consumer's identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should you wish to place a fraud alert, please contact any one of the agencies listed below:

Experian
P.O. Box 9554
Allen, TX 75013
1-888-397-3742
www.experian.com/fraud/center.html

TransUnion
P.O. Box 2000
Chester, PA 19016
1-800-680-7289
www.transunion.com/fraud-victim-resource/place-fraud-alert

Equifax
P.O. Box 105069
Atlanta, GA 30348
1-888-766-0008
www.equifax.com/personal/credit-report-services

What You Can Do. You can find out more about how to protect against potential identity theft and fraud in the enclosed *Steps You Can Take to Help Protect Your Information.* We encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements and explanations of benefits, and to monitor your credit reports for suspicious activity.

For More Information. If you have additional questions, please call our dedicated assistance line at 1-866-938-0442, Monday through Friday (excluding U.S. holidays), during the hours of 8:00 a.m. to 5:00 p.m., Pacific Time (excluding U.S. holidays). You may also write to Assured at 7717 N. Hartman Lane, Tucson, AZ 85743.

We sincerely regret any inconvenience or concern this incident may cause.

Sincerely,

Kyle J. Dulock
Chief Privacy Officer
Assured Imaging

EXHIBIT C

assuredimaging
women's wellness

August 31, 2020

Geraldine Pineda
[redacted]
Las Cruces, NM [redacted]

Re: Notice of Data Breach

Dear Geraldine Pineda:

Assured Imaging ("Assured") is writing to inform you of a recent event that may impact the security of some of your information. Although we are unaware of any actual misuse of your information, we are providing you with information about the event, our response, and steps you may take to better protect against the possibility of identity theft and fraud, should you feel it is necessary to do so.

What Happened? On May 19, 2020, Assured learned that its electronic medical records system had become encrypted due to "ransomware" deployed by an unknown actor. Because the impacted systems contained patient information, Assured worked quickly to (1) restore access to the patient information so it could continue to care for patients without disruption and (2) investigate what happened and whether this incident resulted in any unauthorized access to, or theft of, patient information by the unknown actor.

Assured conducted an extensive investigation, with the assistance of third-party computer forensic specialists to determine the nature and scope of the incident. On July 1, 2020, the investigation confirmed Assured systems were accessible by an unknown actor between May 15, 2020 and May 17, 2020, and certain, limited data was exfiltrated from our systems. The investigation was unable to determine the full extent of information that was accessed by the unknown actor. In an abundance of caution, we performed a comprehensive review of all information stored in our systems at the time of incident to identify the individuals whose information may have been accessible to the unknown actor. We then worked to determine the identities and contact information for potentially impacted individuals.

What Information Was Involved. We determined the following types of information relating to you were present in the electronic medical records system and therefore potentially accessed by the unknown actor during this incident: full name, address, date of birth, patient ID, facility, treating clinician, medical history, service performed, and assessment of the service performed, including any recommendations on future testing. We are unaware that any of this information was misused by the unknown actor and Assured is providing this notice in an abundance of caution.

What We Are Doing. We take this incident and the security of your personal information seriously. Upon learning of this incident, we immediately took steps to restore our operations and further secure our systems. As part of our ongoing commitment to the privacy of personal information in our care, we are working to review our existing policies and procedures and to implement additional safeguards to further secure the information in our systems. Assured also notified the U.S. Department of Health and Human Services and other government regulators, as required.

EXHIBIT D

Privacy Notice to Patients

Patient Handout

Disclosure of Medical Records

1. **Your health information may be used by staff or disclosed to other healthcare professionals for evaluation of your medical health, diagnosis, testing and treatment.**
2. **Your health information may be used to request payment from insurance or other type companies.**
3. **Your health information may be disclosed to law enforcement agencies, federal, state or local agencies to support audits or comply with mandated reporting.**
4. **Your health information may be disclosed to public health agencies as required by law.**

Patient Rights

1. **The right to a copy of this notice.**
2. **The right to request an accounting of how and to whom your information has been disclosed.**
3. **The right to request restrictions on the use and disclosure of your health information.**
4. **The right to receive confidential information concerning your medical condition.**
5. **The right to submit corrections to your health information.**
6. **The right to inspect and/or copy your health information.**
7. **The right to submit a complaint or comment about these rights.**

Assured Imaging Women's Wellness **Attn: Erin Edwards** **7717 N. Hartman Lane** **Tucson, AZ 85743** **(888) 233-6121** **Fax: (520) 572-7138**	**Assistant Director,** **Breast Imaging Accreditation Programs** **American College of Radiology** **1891 Preston White Drive** **Reston, VA 20191-4397** **Fax: (703) 648-9176** **mamm-accred@acr.org**

Patient Rights and Responsibilities
Patient Handout

Your Rights:

- The right to considerate and respectful care, regardless of race, color, religion, sex, age, physical or mental handicap, or national origin.
- The right to communicate with family members and / or significant others.
- The right to a quiet, restful and healing environment.
- The right to agree to treatment before your physician begins any procedure or test.
- The right to know about any specific procedure or treatment, including possible risks.
- The right to complete, up-to-date information about any specific procedure or treatment, including possible risks.
- The right to make decisions with your physician about your health care.
- The right to accept or refuse care as permitted by law.
- The right to prepare a Living Will and / or appoint a person to make healthcare decisions for you as permitted by law.
- The right to have your legally authorized representative make healthcare decisions for you if you become incompetent according to law, or if your physician decides that you can not understand any proposed treatment(s) or procedure(s), or if you can not communicate your wishes regarding your treatment(s).
- The right to know that you will not be discriminated against or your treatment limited based upon whether or not you decide to prepare a living will or durable power of attorney.
- The right to participate in discussions about any ethical issues affecting your care.
- We will discuss your case or exam only with healthcare providers caring for you.
- The right to the privacy of your medical records. Without your consent, we will not release your medical record unless authorized by law or to those responsible for paying your bill.
- The right to restrict the release of your medical information.
- The right to receive an explanation of your bill, regardless of the source of payment.
- The right to express concerns about any aspect of your care without fear of retaliation.
- The right to receive your medical records via your indicated referral contact (physician or self) within 30 days (upon request).
- The right to receive a result letter directly within 30 days

Your Responsibilities:

- Provide your physician and the staff complete and accurate information about your condition and care.
- Follow your physician and staff's orders, instructions regarding your care.
- Accept responsibility for refusing treatment or not following your physician's orders.
- Be considerate of other patients.
- Supply insurance information and pay your bill promptly so we can continue to serve you and the community effectively.

We care about our patients:

Assured Imaging is committed to providing excellent healthcare. We would like to encourage you to return for your follow up visits. If your health was compromised in any way or if there are any unresolved issues regarding Assured Imaging, please contact the accrediting bodies of mammography by writing or calling the following facilities:

Assured Imaging
Attn: Erin Edwards
7717 N. Hartman Lane
Tucson, AZ 85743
(888) 233-6121

Assistant Director, Breast Imaging
Accreditation Programs
American College of Radiology
1891 Preston White Drive
Reston, VA 20191-4397
Fax: (703) 648-9176
mamm-accred@acr.org

EXHIBIT E

Rezolut - HIPAA Website Notice

August 26, 2020 – Assured Imaging ("Assured") is issuing notice of a recent data security event that may impact the confidentiality and security of personal information of certain Assured patients. Although Assured is unaware of any actual misuse of this information, we are providing information about the event, our response, and steps affected individuals may take to better protect against the possibility of identity theft and fraud, should affected individuals feel it is necessary to do so.

What Happened? On May 19, 2020, Assured learned that its electronic medical records system had become encrypted due to "ransomware" deployed by an unknown actor. Because the impacted systems contained patient information, Assured worked quickly to (1) restore access to the patient information so it could continue to care for patients without disruption and (2) investigate what happened and whether this incident resulted in any unauthorized access to, or theft of, patient information by the unknown actor.

Assured conducted an extensive investigation, with the assistance of third-party computer forensic specialists to determine the nature and scope of the incident. On July 1, 2020, the investigation confirmed Assured systems were accessible by an unknown actor between May 15, 2020 and May 17, 2020, and certain, limited data was exfiltrated from our systems. The investigation was unable to determine the full extent of information that was accessed by the unknown actor. In an abundance of caution, Assured performed a comprehensive review of all information stored in our systems at the time of incident to identify the individuals whose information may have been accessible to the unknown actor. We then worked to determine the identities and contact information for potentially impacted individuals.

What Information was Affected. The following types of patient information were present in the electronic medical records system and therefore potentially accessed and acquired by the unknown actor during this incident during the incident: full name, address, date of birth, patient ID, facility, treating clinician, medical history, service performed, and assessment of the service performed, including any recommendations on future testing. We are unaware that any of the information was misused by the unknown actor and Assured is providing this notice in an abundance of caution.

What We are Doing. Assured takes this incident and the security of your personal information seriously. Upon learning of this incident, we immediately took steps to restore our operations and further secure our systems. As part of our ongoing commitment to the privacy of personal information in our care, we are working to review our existing policies and procedures and to implement additional safeguards to further secure the information in our systems. Assured also notified the U.S. Department of Health and Human Services and other government regulators, as required.

What Affected Individuals Can Do. While we are unaware of any misuse of any personal information contained within the impacted system, individuals are encouraged to remain vigilant against incidents of identity theft by reviewing account statements and explanations of benefits for unusual activity and report any suspicious activity immediately to your insurance company, health care provider, or financial institution. Additional detail can be found below, in the *Steps You Can Take to Protect Your Information.*

For More Information. If you have additional questions, please call our dedicated assistance line at 866-938-0442, Monday through Friday (excluding U.S. holidays), during the hours of 8:00 a.m. to 5:00 p.m., Pacific Time (excluding U.S. holidays). You may also write to Assured at 7717 N. Hartman Lane, Tucson, AZ 85743

Steps You Can Take To Protect Your Information

While we are unaware of any misuse of the personal information in the affected system, we encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements, and to monitor your credit reports for suspicious activity. Under U.S. law you are entitled to one free credit report annually from each of the three major credit reporting bureaus. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also contact the three major credit bureaus directly to request a free copy of your credit report.

You have the right to place a "security freeze" on your credit report, which will prohibit a consumer reporting agency from releasing information in your credit report without your express authorization. The security freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a security freeze to take control over who gets access to the personal and financial information in your credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, you cannot be charged to place or lift a security freeze on your credit report. Should you wish to place a security freeze, please contact the major consumer reporting agencies listed below:

Experian	**TransUnion**	**Equifax**
P.O. Box 9554	P.O. Box 160	P.O. Box 105788
Allen, TX 75013	Woodlyn, PA 19094	Atlanta, GA 30348
1-888-397-3742	1-888-909-8872	1-800-685-1111
www.experian.com/freeze/center.html	www.transunion.com/credit-freeze	www.equifax.com/personal/credit-report-services

In order to request a security freeze, you will need to provide the following information:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. If you have moved in the past five (5) years, provide the addresses where you have lived over the prior five years;
5. Proof of current address, such as a current utility bill or telephone bill;
6. A legible photocopy of a government-issued identification card (state driver's license or ID card, military identification, etc.);
7. If you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft.

As an alternative to a security freeze, you have the right to place an initial or extended "fraud alert" on your file at no cost. An initial fraud alert is a 1-year alert that is placed on a consumer's credit file. Upon seeing a fraud alert display on a consumer's credit file, a business is required to take steps to verify the consumer's identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should you wish to place a fraud alert, please contact any one of the agencies listed below:

Experian	**TransUnion**	**Equifax**
P.O. Box 9554	P.O. Box 2000	P.O. Box 105069
Allen, TX 75013	Chester, PA 19016	Atlanta, GA 30348
1-888-397-3742	1-800-680-7289	1-888-766-0008
www.experian.com/fraud/center.html	www.transunion.com/fraud-victim-resource/place-fraud-alert	www.equifax.com/personal/credit-report-services

You can further educate yourself regarding identity theft, fraud alerts, security freezes, and the steps you can take to protect yourself by contacting the consumer reporting agencies, the Federal Trade Commission, or your state Attorney General.

The Federal Trade Commission can be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580, www.identitytheft.gov, 1-877-ID-THEFT (1-877-438-4338); TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. You can obtain further information on how to file such a complaint by way of the contact information listed above. You have the right to file a police report if you ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and your state Attorney General. This notice has not been delayed by law enforcement.

For Maryland residents: The Attorney General can be contacted at 200 St. Paul Place, 16th Floor, Baltimore, MD 21202, 1-410-528-8662, www.oag.state.md.us.

For North Carolina residents: The Attorney General can be contacted at 9001 Mail Service Center, Raleigh, NC 27699-9001, 1-877-566-7226 or 1-919-716-6000, www.ncdoj.gov. You can obtain information from the Attorney General or the Federal Trade Commission about preventing identity theft.

For New Mexico residents: You have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit "prescreened" offers of credit and insurance you get based on information in your credit report; and you may seek damages from violator. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. We encourage you to review your rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

For Rhode Island residents: The Rhode Island Attorney General can be reached at: 150 South Main Street, Providence, Rhode Island 02903; www.riag.ri.gov, 1-401-274-4400. Under Rhode Island law, you have the right

to obtain any police report filed in regard to this incident. There are 4 Rhode Island residents impacted by this incident.

For New York residents: The Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; https://ag.ny.gov/.

For Washington, D.C. residents: The Attorney General may be contacted at Office of the Attorney General, 441 4th Street, NW, Washington, DC 20001; (202) 727-3400; and www.oag@dc.gov.