

James E. Magleby (7247)

[magleby@mcg.law](mailto:magleby@mcg.law)

Jennifer Fraser Parrish (11207)

[parrish@mcg.law](mailto:parrish@mcg.law)

MAGLEBY CATAXINOS & GREENWOOD, PC

141 West Pierpont Avenue

Salt Lake City, Utah 84101

Telephone: 801.359.9000

Facsimile: 801.359.9011

Attorneys for Plaintiff Jerry Lukens

**IN THE THIRD JUDICIAL DISTRICT COURT  
SALT LAKE COUNTY, STATE OF UTAH**

**JERRY LUKENS, individually and on  
behalf of all others similarly situated,**

**Plaintiff,**

**v.**

**UTAH IMAGING ASSOCIATES, INC., a  
Utah corporation,**

**Defendant.**

**CLASS ACTION COMPLAINT**

**JURY TRIAL DEMANDED**

**TIER 3**

**Case No. 210906618  
Honorable Laura Scott**

**CLASS ACTION COMPLAINT**

Plaintiff Jerry Lukens (“Plaintiff”), individually and on behalf of all others similarly situated (collectively, “Class members”), by and through his attorneys, brings this Class Action Complaint against Defendant Utah Imaging Associates, Inc. (“UIA”) and complains and alleges upon personal knowledge as to himself and information and belief as to all other matters.

**INTRODUCTION**

1. Plaintiff brings this class action against UIA for its failure to secure and safeguard his and approximately 583,642 other individuals’ private and confidential medical information,

including names, mailing addresses, dates of birth, Social Security numbers, health insurance policy numbers, and medical information (“PII/PHI”).

2. Defendant is a Utah corporation with its principal place of business in Utah, that provides radiology services throughout Utah. The company provides both off-site and on-site services.

3. On or about September 4, 2021, UIA discovered that unauthorized individuals had gained access to UIA’s network systems and had access to the PII/PHI of Plaintiff and Class members (the “Data Breach”).

4. UIA owed a duty to Plaintiff and Class members to implement and maintain reasonable and adequate security measures to secure, protect, and safeguard their PII/PHI against unauthorized access and disclosure. UIA breached that duty by, among other things, failing to implement and maintain reasonable security procedures and practices to protect its patients’ PII/PHI from unauthorized access and disclosure.

5. As a result of UIA’s inadequate security and breach of its duties and obligations, the Data Breach occurred, and Plaintiff’s and Class members’ PII/PHI was accessed and disclosed. This action seeks to remedy these failings and their consequences. Plaintiff brings this action on behalf of himself and all Utah residents whose PII/PHI was exposed as a result of the Data Breach, which UIA learned of on or about September 4, 2021 and first publicly acknowledged on or about November 18, 2021.

6. Plaintiff, on behalf of himself and all other Class members, asserts claims for negligence, negligence per se, breach of fiduciary duty, breach of implied contract, unjust enrichment, violation of the Utah Consumer Sales Act, and seeks declaratory relief, injunctive

relief, monetary damages, statutory damages, punitive damages, equitable relief, and all other relief authorized by law.

### **PARTIES**

7. Plaintiff Jerry Lukens is a Utah resident. He provided his PII/PHI to UIA in connection with receiving health care services from UIA. He received a letter from UIA notifying him that his PII/PHI may have been exposed in the Data Breach. Had Plaintiff Lukens known that UIA does not adequately protect PII/PHI, he would not have used UIA's services and agreed to provide UIA with his PII/PHI.

8. Defendant Utah Imaging Associates, Inc. is a corporation incorporated in Utah and is located in and around Farmington, Utah. UIA's corporate headquarters are located at 1433 North 1075 West, Suite 104, Farmington, UT 84025.

### **JURISDICTION AND VENUE**

9. This Court has jurisdiction over this action pursuant to Utah Code § 78A-5-102. This action is brought as a class action on behalf of Plaintiff and all Class members pursuant to Utah R. Civ. P. 23 and Utah Code § 13-11-20.

10. This Court has personal jurisdiction over UIA because UIA is a corporation organized under the laws of Utah and has its principal place of business at 1433 North 1075 West, Suite 104, Farmington, UT 84025.

11. Venue is proper in the Third Judicial District pursuant to Utah Code § 78B-3-307 because the causes of action arose in, and Plaintiff resides in, Salt Lake County, Utah.

12. Because Plaintiff and Class members seek monetary relief in excess of \$300,000, this is a Tier 3 action. See Utah R. Civ. P. 26(c)(3).

## **FACTUAL ALLEGATIONS**

### ***Overview of UIA***

13. UIA is a corporation that provides various radiology services for health care providers. UIA offers “diagnostic and interventional imaging services along the Wasatch Front.”<sup>1</sup>

14. In the regular course of its business, UIA collects and maintains the PII/PHI of patients, former patients, and other persons to whom it is currently providing or previously provided health-related or other services.

15. UIA requires patients to provide personal information before it provides them services. That information includes, *inter alia*, names, addresses, dates of birth, health insurance information, and Social Security numbers. UIA stores this information digitally.

16. Plaintiff and Class members are, or were, patients of UIA or received health-related or other services from UIA, and entrusted UIA with their PII/PHI.

### ***The Data Breach***

17. On or about September 4, 2021, UIA discovered that an unauthorized individual, or unauthorized individuals, gained access to UIA’s network systems. UIA has not revealed how long cybercriminals may have had access to its network.

18. UIA began to notify patients about the data breach on or about November 18, 2021. The letters that UIA sent to Plaintiff and the Class state that the information that was accessed included:

“[F]irst and last name; mailing address; date of birth; Social Security number; health insurance policy number; medical information, including, but not limited to, medical treatment, diagnosis, and prescription information.”<sup>2</sup>

---

<sup>1</sup> See Utah Imaging Associates, *About Us*, UTAHIMAGING.COM, <https://www.utahimaging.com/about.html> (last visited Nov. 30, 2021).

<sup>2</sup> Utah Imaging Associates, *Notice of Data Breach*, OAG.CA.GOV,

### *UIA Knew that Criminals Target PII/PHI*

19. At all relevant times, UIA knew, or should have known, its patients', Plaintiff's, and all other Class members' PII/PHI was a target for malicious actors. Despite such knowledge, UIA failed to implement and maintain reasonable and appropriate data privacy and security measures to protect Plaintiff's and Class members' PII/PHI from cyber-attacks that UIA should have anticipated and guarded against.

20. Cyber criminals seek out PHI at a greater rate than other sources of personal information. In a 2021 report, the healthcare compliance company Protenu found that there were 758 medical data breaches in 2020 with over 40 million patient records exposed.<sup>3</sup> This is an increase from the 572 medical data breaches that Protenu compiled in 2019.<sup>4</sup>

21. PII/PHI is a valuable property right.<sup>5</sup> The value of PII/PHI as a commodity is measurable.<sup>6</sup> "Firms are now able to attain significant market valuations by employing business models predicated on the successful use of personal data within the existing legal and regulatory frameworks."<sup>7</sup> American companies are estimated to have spent over \$19 billion on acquiring

---

<https://oag.ca.gov/system/files/UIA%20-%20Notice%20Letter%20-%20Patients%20-%20General%20-%20IDX%20v2.pdf> (last accessed Nov. 30, 2021).

<sup>3</sup> Protenu, *2021 Breach Barometer*, PROTENU.COM, <https://www.protenu.com/resources/2021-breach-barometer> (last accessed Nov. 15, 2021).

<sup>4</sup> Protenu, *2020 Breach Barometer*, PROTENU.COM, <https://www.protenu.com/resources/2020-breach-barometer> (last accessed Nov. 15, 2021).

<sup>5</sup> See Marc van Lieshout, *The Value of Personal Data*, 457 International Federation for Information Processing 26 (May 2015) ("The value of [personal] information is well understood by marketers who try to collect as much data about personal conducts and preferences as possible..."),

[https://www.researchgate.net/publication/283668023\\_The\\_Value\\_of\\_Personal\\_Data](https://www.researchgate.net/publication/283668023_The_Value_of_Personal_Data)

<sup>6</sup> See Robert Lowes, *Stolen EHR [Electronic Health Record] Charts Sell for \$50 Each on Black Market*, MEDSCAPE.COM (April 28, 2014), <http://www.medscape.com/viewarticle/824192>.

<sup>7</sup> OECD, *Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value*, OECD ILIBRARY (April 2, 2013), [https://www.oecd-ilibrary.org/science-and-technology/exploring-the-economics-of-personal-data\\_5k486qtxldmq-en](https://www.oecd-ilibrary.org/science-and-technology/exploring-the-economics-of-personal-data_5k486qtxldmq-en).

personal data of consumers in 2018.<sup>8</sup> It is so valuable to identity thieves that once PII/PHI has been disclosed, criminals often trade it on the “cyber black-market,” or the “dark web,” for many years.

22. As a result of its real value and the recent large-scale data breaches, identity thieves and cyber criminals have openly posted credit card numbers, SSNs, PII/PHI, and other sensitive information directly on various Internet websites making the information publicly available. This information from various breaches, including the information exposed in the Data Breach, can be aggregated and become more valuable to thieves and more damaging to victims.

23. PHI is particularly valuable and has been referred to as a “treasure trove for criminals.”<sup>9</sup> A cybercriminal who steals a person’s PHI can end up with as many as “seven to ten personal identifying characteristics of an individual.”<sup>10</sup> A study by Experian found that the “average total cost” of medical identity theft is “about \$20,000” per incident, and that a majority of victims of medical identity theft were forced to pay out-of-pocket costs for healthcare they did not receive in order to restore coverage.<sup>11</sup>

24. All-inclusive health insurance dossiers containing sensitive health insurance information, names, addresses, telephone numbers, email addresses, SSNs, and bank account information, complete with account and routing numbers, can fetch up to \$1,200 to \$1,300 each

---

<sup>8</sup> IAB Data Center of Excellence, *U.S. Firms to Spend Nearly \$19.2 Billion on Third-Party Audience Data and Data-Use Solutions in 2018, Up 17.5% from 2017*, IAB.COM (Dec. 5, 2018), <https://www.iab.com/news/2018-state-of-data-report/>.

<sup>9</sup> See Andrew Steager, *What Happens to Stolen Healthcare Data*, HEALTHTECH MAGAZINE (Oct. 20, 2019), <https://healthtechmagazine.net/article/2019/10/what-happens-stolen-healthcare-data-perfcon> (“*What Happens to Stolen Healthcare Data Article*”) (quoting Tom Kellermann, Chief Cybersecurity Officer, Carbon Black, stating “Health information is a treasure trove for criminals.”).

<sup>10</sup> *Id.*

<sup>11</sup> See Elinor Mills, *Study: Medical identity theft is costly for victims*, CNET (Mar. 3, 2010), <https://www.cnet.com/news/study-medical-identity-theft-is-costly-for-victims>.

on the black market.<sup>12</sup> According to a report released by the Federal Bureau of Investigation’s (“FBI”) Cyber Division, criminals can sell healthcare records for 50 times the price of a stolen Social Security or credit card number.<sup>13</sup>

25. Criminals can use stolen PII/PHI to extort a financial payment by “leveraging details specific to a disease or terminal illness.”<sup>14</sup> Quoting Carbon Black’s Chief Cybersecurity Officer, one recent article explained: “Traditional criminals understand the power of coercion and extortion . . . By having healthcare information—specifically, regarding a sexually transmitted disease or terminal illness—that information can be used to extort or coerce someone to do what you want them to do.”<sup>15</sup>

26. Consumers place a high value on the privacy of that data. Researchers shed light on how much consumers value their data privacy—and the amount is considerable. Indeed, studies confirm that “when privacy information is made more salient and accessible, some consumers are willing to pay a premium to purchase from privacy protective websites.”<sup>16</sup>

27. Given these facts, any company that transacts business with a consumer and then compromises the privacy of consumers’ PII/PHI has thus deprived that consumer of the full monetary value of the consumer’s transaction with the company.

---

<sup>12</sup> SC Staff, *Health Insurance Credentials Fetch High Prices in the Online Black Market*, SC MAGAZINE (July 16, 2013), <https://www.scmagazine.com/news/breach/health-insurance-credentials-fetch-high-prices-in-the-online-black-market>.

<sup>13</sup> Federal Bureau of Investigation, *Health Care Systems and Medical Devices at Risk for Increased Cyber Intrusions for Financial Gain* (April 8, 2014), <https://www.illumweb.com/wp-content/uploads/ill-mo-uploads/103/2418/health-systems-cyber-intrusions.pdf>.

<sup>14</sup> *What Happens to Stolen Healthcare Data*, *supra* at n.10.

<sup>15</sup> *Id.*

<sup>16</sup> Janice Y. Tsai et al., *The Effect of Online Privacy Information on Purchasing Behavior, An Experimental Study*, 22(2) INFORMATION SYSTEMS RESEARCH 254 (June 2011) <https://www.jstor.org/stable/23015560?seq=1>.

### *Theft of PII/PHI Has Grave and Lasting Consequences for Victims*

28. Theft of PII/PHI is serious. The FTC warns consumers that identity thieves use PII/PHI to exhaust financial accounts, receive medical treatment, start new utility accounts, and incur charges and credit in a person's name.<sup>17</sup>

29. Identity thieves use personal information for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud.<sup>18</sup> According to Experian, one of the largest credit reporting companies in the world, “[t]he research shows that personal information is valuable to identity thieves, and if they can get access to it, they will use it” to among other things: open a new credit card or loan; change a billing address so the victim no longer receives bills; open new utilities; obtain a mobile phone; open a bank account and write bad checks; use a debit card number to withdraw funds; obtain a new driver's license or ID; use the victim's information in the event of arrest or court action.<sup>19</sup>

30. With access to an individual's PII/PHI, criminals can do more than just empty a victim's bank account—they can also commit all manner of fraud, including: obtaining a driver's license or official identification card in the victim's name but with the thief's picture; using the

---

<sup>17</sup> See Federal Trade Commission, *What to Know About Identity Theft*, FEDERAL TRADE COMMISSION CONSUMER INFORMATION, <https://www.consumer.ftc.gov/articles/what-know-about-identity-theft> (last accessed Nov. 15, 2021).

<sup>18</sup> The FTC defines identity theft as “a fraud committed or attempted using the identifying information of another person without authority.” 16 C.F.R. § 603.2. The FTC describes “identifying information” as “any name or number that may be used, alone or in conjunction with any other information, to identify a specific person,” including, among other things, “[n]ame, social security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number. *Id.*”

<sup>19</sup> See Susan Henson, *What Can Identity Thieves Do with Your Personal Information and How Can You Protect Yourself*, EXPERIAN (Sept. 1, 2017), <https://www.experian.com/blogs/ask-experian/what-can-identity-thieves-do-with-your-personal-information-and-how-can-you-protect-yourself/>.



victim's name and SSN to obtain government benefits; or, filing a fraudulent tax return using the victim's information. In addition, identity thieves may obtain a job using the victim's SSN, 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.<sup>20</sup>

31. Identity theft is not an easy problem to solve. In a survey, the Identity Theft Resource Center found that most victims of identity crimes need more than a month to resolve issues stemming from identity theft and some need over a year.<sup>21</sup>

32. Theft of SSNs also creates a particularly alarming situation for victims because those numbers cannot easily be replaced. In order to obtain a new number, a breach victim has to demonstrate ongoing harm from misuse of her SSN, and a new SSN will not be provided until after the harm has already been suffered by the victim.

33. Due to the highly sensitive nature of SSNs, theft of SSNs in combination with other PII (e.g., name, address, date of birth) is akin to having a master key to the gates of fraudulent activity. TIME quotes data security researcher Tom Stickley, who is employed by companies to find flaws in their computer systems, as stating, "If I have your name and your Social Security number and you don't have a credit freeze yet, you're easy pickings."<sup>22</sup>

34. Theft of PII is even more serious when it includes theft of PHI. Data breaches

---

<sup>20</sup> See Federal Trade Commission, *Warning Signs of Identity Theft*, IDENTITYTHEFT.GOV <https://www.identitytheft.gov/Warning-Signs-of-Identity-Theft> (last accessed Nov. 15, 2021).

<sup>21</sup> Identity Theft Resource Center, *2021 Consumer Aftermath Report*, IDENTITY THEFT RESOURCE CENTER (2021), <https://www.idtheftcenter.org/identity-theft-aftermath-study/> (last accessed Nov. 15, 2021).

<sup>22</sup> Patrick Lucas Austin, *'It Is Absurd.' Data Breaches Show it's Time to Rethink How We Use Social Security Numbers, Experts Say*, TIME (August 5, 2019), <https://time.com/5643643/capital-one-equifax-data-breach-social-security/>.

involving medical information “typically leave[] a trail of falsified information in medical records that can plague victims’ medical and financial lives for years.”<sup>23</sup> It “is also more difficult to detect, taking almost twice as long as normal identity theft.”<sup>24</sup> In warning consumers on the dangers of medical identity theft, the FTC states that an identity thief may use PII/PHI “to see a doctor, get prescription drugs, buy medical devices, submit claims with your insurance provider, or get other medical care.”<sup>25</sup> The FTC also warns, “If the thief’s health information is mixed with yours, your treatment, insurance and payment records, and credit report may be affected.”<sup>26</sup>

35. A report published by the World Privacy Forum and presented at the US FTC Workshop on Informational Injury describes what medical identity theft victims may experience:

- Changes to their health care records, most often the addition of falsified information, through improper billing activity or activity by imposters. These changes can affect the healthcare a person receives if the errors are not caught and corrected.
- Significant bills for medical goods and services not sought nor received.
- Issues with insurance, co-pays, and insurance caps.
- Long-term credit problems based on problems with debt collectors reporting debt due to identity theft.
- Serious life consequences resulting from the crime; for example, victims have been falsely accused of being drug users based on falsified entries to their medical files; victims have had their children removed from them due to medical activities of the imposter; victims have been denied jobs due to incorrect information placed in their health files due to the crime.

---

<sup>23</sup> Pam Dixon and John Emerson, *The Geography of Medical Identity Theft*, FTC.GOV (Dec. 12, 2017), [https://www.ftc.gov/system/files/documents/public\\_comments/2018/01/00037-142815.pdf](https://www.ftc.gov/system/files/documents/public_comments/2018/01/00037-142815.pdf)

<sup>24</sup> See Federal Bureau of Investigation, *Health Care Systems and Medical Devices at Risk...*, *supra* at n.14.

<sup>25</sup> See Federal Trade Commission, *What to Know About Medical Identity Theft*, Federal Trade Commission Consumer Information, <https://www.consumer.ftc.gov/articles/what-know-about-medical-identity-theft> (last accessed Nov. 15, 2021).

<sup>26</sup> *Id.*

- As a result of improper and/or fraudulent medical debt reporting, victims may not qualify for mortgage or other loans and may experience other financial impacts.
- Phantom medical debt collection based on medical billing or other identity information.
- Sales of medical debt arising from identity theft can perpetuate a victim's debt collection and credit problems, through no fault of their own.<sup>27</sup>

36. There may also be a time lag between when sensitive personal information is stolen, when it is used, and when a person discovers it has been used. For example, on average it takes approximately three months for consumers to discover their identity has been stolen and used and it takes some individuals up to three years to learn that information.<sup>28</sup>

37. It is within this context that Plaintiff and all other Class members must now live with the knowledge that their PII/PHI is forever in cyberspace and was taken by people willing to use the information for any number of improper purposes and scams, including making the information available for sale on the black-market.

***Damages Sustained by Plaintiff and the Other Class Members***

38. Plaintiff and all other Class members have suffered injury and damages, including, but not limited to: (i) a substantially increased risk of identity theft and medical theft—risks justifying expenditures for protective and remedial services for which they are entitled to compensation; (ii) improper disclosure of their PII/PHI; (iii) breach of the confidentiality of their PII/PHI; (iv) deprivation of the value of their PII/PHI, for which there is a well-established national and international market; and/or (v) lost time and money incurred to mitigate and remediate the

---

<sup>27</sup> See Pam Dixon and John Emerson, *The Geography of Medical Identity Theft*, *supra* at 24.

<sup>28</sup> John W. Coffey, *Difficulties in Determining Data Breach Impacts*, 17 *Journal of Systemics, Cybernetics and Informatics* 9 (2019), <http://www.iiisci.org/journal/pdv/sci/pdfs/IP069LL19.pdf>.

effects of the Data Breach, including the increased risks of identity theft and medical identity theft they face and will continue to face.

### **CLASS ALLEGATIONS**

39. This action is brought and may be properly maintained as a class action pursuant to Utah R. Civ. P. 23.

40. Plaintiff brings this action on behalf of himself and all members of the following Class of similarly situated persons:

All Utah residents whose PHI/PII was accessed by and disclosed to unauthorized persons in the Data Breach, including all Utah residents who were sent a notice of the Data Breach.

41. Excluded from the Class is UIA and its affiliates, parents, subsidiaries, officers, agents, and directors, as well as the judge(s) presiding over this matter and the clerks of said judge(s).

42. Certification of Plaintiff's claims for class-wide treatment is appropriate because Plaintiff can prove the elements of his claims on a class-wide basis using the same evidence as would be used to prove those elements in individual actions alleging the same claims.

43. The members in the Class are so numerous that joinder of all Class members in a single proceeding would be impracticable. UIA reported to the U.S. Department of Health and Human Services' Office of Civil Rights that approximately 583,643 individuals' information was exposed in the Data Breach.

44. Common questions of law and fact exist as to all Class members and predominate over any potential questions affecting only individual Class members. Such common questions of law or fact include, *inter alia*:

- a. Whether UIA had a duty to implement and maintain reasonable security procedures and practices to protect and secure Plaintiff's and Class Members' PII/PHI from unauthorized access and disclosure;
- b. Whether UIA failed to exercise reasonable care to secure and safeguard Plaintiff's and Class Members' PII/PHI;
- c. Whether an implied contract existed between Class members and UIA providing that UIA would implement and maintain reasonable security measures to protect and secure Class members' PII/PHI from unauthorized access and disclosure;
- d. Whether UIA breached its duties to protect Plaintiff's and Class members' PII/PHI; and
- e. Whether Plaintiff and all other members of the Class are entitled to damages and the measure of such damages and relief.

45. UIA engaged in a common course of conduct giving rise to the legal rights sought to be enforced by Plaintiff on behalf of himself and all other Class members. Individual questions, if any, pale in comparison, in both quantity and quality, to the numerous common questions that dominate this action.

46. Plaintiff's claims are typical of the claims of the Class. Plaintiff, like all proposed members of the Class, had his PII/PHI compromised in the Data Breach. Plaintiff and Class members were injured by the same wrongful acts, practices, and omissions committed by UIA, as described herein. Plaintiff's claims therefore arise from the same practices or course of conduct that give rise to the claims of all Class members.

47. Plaintiff will fairly and adequately protect the interests of the Class members. Plaintiff is an adequate representative of the Class in that he has no interests adverse to, or that conflict with, the Class he seeks to represent. Plaintiff has retained counsel with substantial experience and success in the prosecution of complex consumer protection class actions of this nature.

48. A class action is superior to any other available means for the fair and efficient adjudication of this controversy, and no unusual difficulties are likely to be encountered in the management of this class action. The damages and other financial detriment suffered by Plaintiff and all other Class members are relatively small compared to the burden and expense that would be required to individually litigate their claims against UIA, so it would be impracticable for Class members to individually seek redress from UIA's wrongful conduct. Even if Class members could afford individual litigation, the court system could not. Individualized litigation creates a potential for inconsistent or contradictory judgments, and increases the delay and expense to all parties and the court system. By contrast, the class action device presents far fewer management difficulties and provides the benefits of single adjudication, economy of scale, and comprehensive supervision by a single court.

## **CAUSES OF ACTION**

### **COUNT I**

#### **NEGLIGENCE**

49. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

50. UIA owed a duty to Plaintiff and all other Class members to exercise reasonable care in safeguarding and protecting their PII/PHI in its possession, custody, or control.

51. UIA knew the risks of collecting and storing Plaintiff's and all other Class members' PII/PHI and the importance of maintaining secure systems. UIA knew of the many data breaches that targeted healthcare providers in recent years.

52. Given the nature of UIA's business, the sensitivity and value of the PII/PHI it maintains, and the resources at its disposal, UIA should have identified the vulnerabilities to their systems and prevented the Data Breach from occurring.

53. UIA breached these duties by failing to exercise reasonable care in safeguarding and protecting Plaintiff's and Class members' PII/PHI by failing to design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems to safeguard and protect PII/PHI entrusted to it—including Plaintiff's and Class members' PII/PHI.

54. It was reasonably foreseeable to UIA that its failure to exercise reasonable care in safeguarding and protecting Plaintiff's and Class members' PII/PHI by failing to design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems would result in the unauthorized release, disclosure, and dissemination of Plaintiff's and Class members' PII/PHI to unauthorized individuals.

55. But for UIA's negligent conduct or breach of the above-described duties owed to Plaintiff and Class members, their PII/PHI would not have been compromised.

56. As a result of UIA's above-described wrongful actions, inaction, and want of ordinary care that directly and proximately caused the Data Breach, Plaintiff and all other Class members have suffered, and will continue to suffer, economic damages and other injury and actual harm in the form of, *inter alia*: (i) a substantially increased risk of identity theft and medical theft—

risks justifying expenditures for protective and remedial services for which they are entitled to compensation; (ii) improper disclosure of their PII/PHI; (iii) breach of the confidentiality of their PII/PHI; (iv) deprivation of the value of their PII/PHI, for which there is a well-established national and international market; and/or (v) lost time and money incurred to mitigate and remediate the effects of the Data Breach, including the increased risks of medical identity theft they face and will continue to face.

## **COUNT II**

### **NEGLIGENCE PER SE**

57. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

58. UIA's duties arise from, *inter alia*, the HIPAA Privacy Rule ("Standards for Privacy of Individually Identifiable Health Information"), 45 C.F.R. Part 160 and Part 164, Subparts A and E, and the HIPAA Security Rule ("Security Standards for the Protection of Electronic Protected Health Information"), 45 C.F.R. Part 160 and Part 164, Subparts A and C (collectively, "HIPAA Privacy and Security Rules").

59. UIA's duties also arise from Section 5 of the FTC Act ("FTCA"), 15 U.S.C. § 45(a)(1), which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted by the FTC, the unfair act or practice by business, such as UIA, of failing to employ reasonable measures to protect and secure PII/PHI.

60. UIA violated HIPAA Privacy and Security Rules and Section 5 of the FTCA by failing to use reasonable measures to protect Plaintiff's and all other Class members' PII/PHI and not complying with applicable industry standards. UIA's conduct was particularly unreasonable given the nature and amount of PII/PHI it obtains and stores, and



the foreseeable consequences of a data breach involving PII/PHI including, specifically, the substantial damages that would result to Plaintiff and the other Class members.

61. UIA's violations of HIPAA Privacy and Security Rules and Section 5 of the FTCA constitutes negligence per se.

62. Plaintiff and Class members are within the class of persons that HIPAA Privacy and Security Rules and Section 5 of the FTCA were intended to protect.

63. The harm occurring as a result of the Data Breach is the type of harm HIPAA Privacy and Security Rules and Section 5 of the FTCA were intended to guard against.

64. It was reasonably foreseeable to UIA that its failure to exercise reasonable care in safeguarding and protecting Plaintiff's and Class members' PII/PHI by failing to design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems, would result in the release, disclosure, and dissemination of Plaintiff's and Class members' PII/PHI to unauthorized individuals.

65. The injury and harm that Plaintiff and the other Class members suffered was the direct and proximate result of UIA's violations of HIPAA Privacy and Security Rules and Section 5 of the FTCA. Plaintiff and Class members have suffered (and will continue to suffer) economic damages and other injury and actual harm in the form of, *inter alia*: (i) a substantially increased risk of identity theft and medical theft—risks justifying expenditures for protective and remedial services for which they are entitled to compensation; (ii) improper disclosure of their PII/PHI; (iii) breach of the confidentiality of their PII/PHI; (iv) deprivation of the value of their PII/PHI, for which there is a well-established national and international market; and/or (v) lost

time and money incurred to mitigate and remediate the effects of the Data Breach, including the increased risks of medical identity theft they face and will continue to face.

### **COUNT III**

#### **BREACH OF FIDUCIARY DUTY**

66. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

67. Plaintiff and Class members gave UIA their PII/PHI in confidence, believing that UIA would protect that information. Plaintiff and Class members would not have provided UIA with this information had they known it would not be adequately protected. UIA's acceptance and storage of Plaintiff's and Class members' PII/PHI created a fiduciary relationship between UIA and Plaintiff and Class members. In light of this relationship, UIA must act primarily for the benefit of its patients, which includes safeguarding and protecting Plaintiff's and Class Members' PII/PHI.

68. UIA has a fiduciary duty to act for the benefit of Plaintiff and Class Members upon matters within the scope of their relationship. It breached that duty by failing to properly protect the integrity of the system containing Plaintiff's and Class Members' PII/PHI, failing to comply with the data security guidelines set forth by HIPAA, and otherwise failing to safeguard Plaintiff's and Class members' PII/PHI that it collected.

69. As a direct and proximate result of UIA's breaches of its fiduciary duties, Plaintiff and Class members have suffered and will suffer injury, including, but not limited to: (i) a substantial increase in the likelihood of identity theft; (ii) the compromise, publication, and theft of their PII/PHI; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from unauthorized use of their PII/PHI; (iv) lost opportunity costs

associated with effort attempting to mitigate the actual and future consequences of the Data Breach; (v) the continued risk to their PII/PHI which remains in UIA's possession; and (vi) future costs in terms of time, effort, and money that will be required to prevent, detect, and repair the impact of the PII/PHI compromised as a result of the Data Breach.

#### **COUNT IV**

##### **BREACH OF IMPLIED CONTRACT**

70. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

71. In connection with receiving medical services, Plaintiff and all other Class members entered into implied contracts with UIA.

72. Pursuant to these implied contracts, Plaintiff and Class members paid money to UIA, whether directly or through their insurers, and provided UIA with their PII/PHI. In exchange, UIA agreed to, among other things, and Plaintiff understood that UIA would: (1) provide medical services to Plaintiff and Class member; (2) take reasonable measures to protect the security and confidentiality of Plaintiff's and Class members' PII/PHI; and (3) protect Plaintiff's and Class members PII/PHI in compliance with federal and state laws and regulations and industry standards.

73. The protection of PII/PHI was a material term of the implied contracts between Plaintiff and Class members, on the one hand, and UIA, on the other hand. Indeed, as set forth *supra*, UIA recognized the importance of data security and the privacy of its patients' PII/PHI in its Privacy Notice. Had Plaintiff and Class members known that UIA would not adequately protect its patients' and former patients' PII/PHI, they would not have received medical services from UIA.

74. Plaintiff and Class members performed their obligations under the implied contract when they provided UIA with their PII/PHI and paid—directly or through their insurers—for health care services from UIA.

75. UIA breached its obligations under its implied contracts with Plaintiff and Class members in failing to implement and maintain reasonable security measures to protect and secure their PII/PHI and in failing to implement and maintain security protocols and procedures to protect Plaintiff's and Class members' PII/PHI in a manner that complies with applicable laws, regulations, and industry standards.

76. UIA's breach of its obligations of its implied contracts with Plaintiff and Class members directly resulted in the Data Breach and the injuries that Plaintiff and all other Class members have suffered from the Data Breach.

77. Plaintiff and all other Class members were damaged by UIA's breach of implied contracts because: (i) they paid—directly or through their insurers—for data security protection they did not receive; (ii) they face a substantially increased risk of identity theft and medical theft—risks justifying expenditures for protective and remedial services for which they are entitled to compensation; (iii) their PII/PHI was improperly disclosed to unauthorized individuals; (iv) the confidentiality of their PII/PHI has been breached; (v) they were deprived of the value of their PII/PHI, for which there is a well-established national and international market; and/or (vi) lost time and money incurred to mitigate and remediate the effects of the Data Breach, including the increased risks of medical identity theft they face and will continue to face.

**COUNT V**

**UNJUST ENRICHMENT**

78. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

79. This claim is pleaded in the alternative to the breach of implied contract claim.

80. Plaintiff and Class members conferred a monetary benefit upon UIA in the form of monies paid for healthcare services or other services.

81. UIA accepted or had knowledge of the benefits conferred upon it by Plaintiff and Class Members. UIA also benefitted from the receipt of Plaintiff's and Class members' PHI, as this was used to facilitate payment.

82. As a result of UIA's conduct, Plaintiff and Class members suffered actual damages in an amount equal to the difference in value between their payments made with reasonable data privacy and security practices and procedures that Plaintiff and Class members paid for, and those payments without reasonable data privacy and security practices and procedures that they received.

83. UIA should not be permitted to retain the money belonging to Plaintiff and Class members because UIA failed to adequately implement the data privacy and security procedures for itself that Plaintiff and Class members paid for and that were otherwise mandated by federal, state, and local laws and industry standards.

84. UIA should be compelled to provide for the benefit of Plaintiff and Class members all unlawful proceeds received by it as a result of the conduct and Data Breach alleged herein.

## COUNT VI

### **VIOLATION OF THE UTAH CONSUMER SALES PRACTICES ACT Utah Code §§ 13-11-1 et seq. (“UCSPA”)**

85. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

86. The UCSPA states, “A deceptive act or practice by a supplier in connection with a consumer transaction violates this chapter whether it occurs before, during, or after the transaction.” Utah Code § 13-11-4(1).

87. UIA is a “supplier,” as defined by Utah Code § 13-11-3(6).

88. Plaintiff and all members of the Class are “person[s]” within the meaning of Utah Code § 13-11-3(5).

89. The medical services that Plaintiff and Class members obtained from UIA constitute a “consumer transaction” as defined in Utah Code § 13-11-3(2).

90. UIA violated the UCSPA through its failure to adequately safeguard and maintain Plaintiff and Class members’ PII/PHI.

91. As a result of UIA’s above-described conduct, Plaintiff and the Class have suffered damages from the disclosure of their information to unauthorized individuals.

92. The injury and harm that Plaintiff and the other Class members suffered was the direct and proximate result of UIA’s violations of the UCSPA. Plaintiff and Class members have suffered (and will continue to suffer) economic damages and other injury and actual harm in the form of, *inter alia*: (i) a substantially increased risk of identity theft and medical theft—risks justifying expenditures for protective and remedial services for which they are entitled to compensation; (ii) improper disclosure of their PII/PHI; (iii) breach of the confidentiality of their PII/PHI; (iv) deprivation of the value of their PII/PHI, for which there is a well-established national

and international market; and/or (v) lost time and money incurred to mitigate and remediate the effects of the Data Breach, including the increased risks of medical identity theft they face and will continue to face.

93. Plaintiff, individually and for each member of the Class, seeks actual damages, injunctive relief, attorneys' fees, litigation expenses, and court costs.

94. In accordance with Utah Code § 13-11-21(2), counsel for Plaintiff will mail by certified mail with return receipt requested a copy of this Complaint to the Utah Division of Consumer Protection.

### **PRAYER FOR RELIEF**

Plaintiff, individually and on behalf of all other members of the Class, respectfully requests that the Court enter judgment in his favor and against UIA as follows:

A. Certifying the Class as requested herein, designating Plaintiff as Class representative, and appointing Plaintiff's counsel as Class Counsel;

B. Awarding Plaintiff and the Class appropriate monetary relief, including actual damages, statutory damages, punitive damages, restitution, and disgorgement;

C. Awarding Plaintiff and the Class equitable, injunctive, and declaratory relief, as may be appropriate. Plaintiff, on behalf of himself and the Class, seeks appropriate injunctive relief designed to prevent UIA from experiencing another data breach by adopting and implementing best data security practices to safeguard PII/PHI and to provide or extend credit monitoring services and similar services to protect against all types of identity theft and medical identity theft;

D. Awarding Plaintiff and the Class pre-judgment and post-judgment interest to the maximum extent allowable;

E. Awarding Plaintiff and the Class reasonable attorneys' fees, costs, and expenses, as allowable; and

F. Awarding Plaintiff and the Class such other favorable relief as allowable under law.

**JURY TRIAL DEMANDED**

Plaintiff demands a trial by jury of all claims in this Class Action Complaint so triable.

Dated: December 8, 2021

Respectfully submitted,



---

JAMES E. MAGLEBY (7247)

[magleby@mcg.law](mailto:magleby@mcg.law)

JENNIFER FRASER PARRISH (11207)

[parish@mcg.law](mailto:parish@mcg.law)

**MAGLEBY CATAXINOS  
& GREENWOOD**

141 W. Pierpont Ave.

Salt Lake City, UT. 84101

Telephone: 801.359.9000

Facsimile: 801.359.9011

TINA WOLFSON\*

[twolfson@ahdootwolfson.com](mailto:twolfson@ahdootwolfson.com)

ROBERT AHDOOT\*

[rahdoot@ahdootwolfson.com](mailto:rahdoot@ahdootwolfson.com)

**AHDOOT & WOLFSON, PC**

2600 W. Olive Avenue, Suite 500

Burbank, CA 91505-4521

Telephone: 310.474.9111

Facsimile: 310.474.8585

ANDREW W. FERICH\*

[aferich@ahdootwolfson.com](mailto:aferich@ahdootwolfson.com)

**AHDOOT & WOLFSON, PC**

201 King of Prussia Road, Suite 650

Radnor, PA 19087

Telephone: 310.474.9111

Facsimile: 310.474.8585



BEN BARNOW\*

[b.barnow@barnowlaw.com](mailto:b.barnow@barnowlaw.com)

ANTHONY L. PARKHILL\*

[aparkhill@barnowlaw.com](mailto:aparkhill@barnowlaw.com)

RILEY W. PRINCE\*

[rprince@barnowlaw.com](mailto:rprince@barnowlaw.com)

**BARNOW AND ASSOCIATES, P.C.**

205 West Randolph Street, Ste. 1630

Chicago, IL 60606

Tel: 312.621.2000

Fax: 312.641.5504

*\*pro hac vice to be submitted*