2nd DISTRICT COURT, COUNTY OF DENVER, STATE OF COLORADO Court Address: 1437 Bannock Street Denver, Colorado 80202 **KRISTEN SNYDER and DIONA LOPEZ, individually and on behalf of all others similarly situated,** **Plaintiffs,** **v.** **THE UROLOGY CENTER OF COLORADO, P.C., a Colorado corporation,** **Defendant.**	▲ **COURT USE ONLY** ▲
Attorneys for Plaintiffs: Rick D. Bailey, Esq. Atty. Reg. #26554 Law Office of Rick D. Bailey, Esq. 1085 Lafayette St., Ste 702 Denver, Colorado 80218 Phone: (720) 676-6023 Email: rick@rickbaileylaw.com David K. Lietz (pro hac vice motion filed and pending) **MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN, PLLC** 5335 Wisconsin Avenue NW Suite 440 Washington, D.C. 20015-2052 Telephone: (866) 252-0878 Facsimile: (202) 686-2877 Email: dlietz@milberg.com Nicholas A. Migliaccio (pro hac vice forthcoming) Jason Rathod (pro hac vice forthcoming) Kevin Leddy (pro hac vice forthcoming) **Migliaccio & Rathod, LLP** 412 H Street NE Washington, D.C. 20002 202.470.3520 nmigliaccio@classlawdc.com	**Case Number: 2021CV33707** **Division 466**
AMENDED CLASS ACTION COMPLAINT AND JURY DEMAND	

Plaintiffs Kristen Snyder and Diona Lopez, individually and on behalf of all others similarly situated, bring this class action lawsuit against Defendant The Urology Center of Colorado ("TUCC" or "Defendant"), a Colorado corporation, to obtain damages, restitution and injunctive relief for the Classes, as defined below. Plaintiffs set forth the following allegations upon information and belief, except as to their own actions, the investigation of their counsel and certain facts that are a matter of public record.

NATURE OF THE ACTION

1. In October of 2021, TUCC publicly announced that it experienced a security incident that caused a disruption to its IT systems.

2. Like so many before it in the healthcare industry, the outage was caused by external threat actors gaining access to TUCC's network between September 7 and September 8, 2021.

3. This attack caused avoidable disruption with Defendant's computer network and enabled an unauthorized third party to access its computer systems and the highly sensitive and confidential data of tens of thousands of current and former patients.

4. According to its Notice of Data Security Incident and its report of the breach to the Department of Health and Human Services Office of Civil Rights, the data security incident that TUCC experienced caused Plaintiffs' and 137,820 other current and former patients' personally identifiable information and protected health information, as defined by the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), including, but not limited to, patients' names, addresses, dates of birth, phone numbers, email addresses, Social Security Numbers, medical record numbers, treating physicians, treating costs, diagnosis, and health insurance

information (collectively, the "Private Information"), to be accessed and compromised by an unauthorized third party (the "Data Breach").[1]

5. As detailed below, the Data Breach was a direct result of Defendant's failure to implement adequate and reasonable cyber-security procedures and protocols necessary to protect Plaintiffs' and the Class Members' Private Information despite the fact that ransomware attacks, which is the believed mechanism of the cyberattack at issue, against medical systems and healthcare providers are at an all-time high.

6. Upon information and belief, the mechanism of the cyberattack and potential for improper disclosure of Plaintiffs' and Class Members' Private Information was a known risk to Defendant, through high news reports and FBI warnings to the healthcare industry, and thus it was on notice that failing to take steps necessary to secure the Private Information from those risks left the property in a dangerous and vulnerable condition.

7. Defendant disregarded the rights of Plaintiffs and Class Members (defined below) by, *inter alia*, intentionally, willfully, recklessly or negligently failing to take adequate and reasonable measures to ensure its data systems were protected against unauthorized intrusions; failing to disclose that it did not have adequately robust computer systems and security practices to safeguard patient Private Information; failing to take standard and reasonably available steps to prevent the Data Breach and failing to provide Plaintiffs and Class Members accurate notice of the Data Breach.

[1] A true and correct copy of TUCC's "Notice of Data Security Incident" is available here: https://www.tucc.com/about-tucc/updates/ (last visited Nov. 18, 2021). The report Defendant submitted to the Department of Health and Human Services' Office for Civil Rights' Breach Portal can be accessed at: https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf (last visited Nov. 18, 2021).

8. In addition, Defendant and its employees failed to properly monitor the computer network and systems that housed the Private Information.

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

10. Armed with the Private Information accessed in the Data Breach, data thieves can commit a variety of crimes including, *e.g.*, opening new financial accounts in Class Members' names, taking out loans in Class Members' names, 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/or giving false information to police during an arrest.

11. As a result of the Data Breach, Plaintiffs and Class Members have been exposed to a substantial and present 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.

12. 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.

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

14. Plaintiffs seek remedies including, but not limited to, compensatory damages, nominal 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.

PARTIES

15. Plaintiff Kristen Snyder is, and at all times mentioned herein was, an individual citizen of the State of Colorado residing in the City of Denver.

16. Plaintiff Snyder, a patient of TUCC, received the notification letter dated November 10, 2021.

17. Plaintiff Diona Lopez is a resident of Denver Colorado. Ms. Lopez was a patient of TUCC several times before the Data Breach event. To receive services at TUCC, Plaintiff Lopez was required to disclose her PII, which was then entered into TUCC's database and maintained by Defendant. In maintaining her information, Defendant expressly and impliedly promised to safeguard Plaintiff Lopez's PII. Defendant, however, did not take proper care of Ms. Lopez's PII, leading to its exposure as a direct result of Defendant's inadequate security measures. In or about October of 2021, Plaintiff Lopez received a notification letter from Defendant stating that her PII was taken, which included her "date of birth, Social Security number, address, phone number, email address, medical record number, diagnosis, treating physician, insurance provider, treatment cost, and/or guarantor name."

18. Defendant TUCC is medical practice group consisting of 20 urologists and radiation oncologists servicing the Denver community.[2]

JURISDICTION & VENUE

19. Jurisdiction is proper in this Court because Plaintiffs are citizens and residents of Denver, Colorado, Defendant TUCC is a Colorado corporation, and Defendant's principal place of business is in Denver, Colorado.

[2] https://www.tucc.com/about-tucc/ (last visited Nov. 18, 2021).

20. Venue is proper in this Court pursuant to Colo. R. Civ. P. 98(c), as a substantial portion of the acts and transactions that constitute the violations of law complained of herein occurred in Denver County, Colorado and Defendant conducts substantial business throughout Denver County.

STATEMENT OF FACTS

Defendant's Business

21. TUCC is a urology center located in Denver, Colorado. Its team of 20 specialized doctors provide treatment for all urologic conditions at its Denver location.[3]

22. The Urology Surgery Center of Colorado (USCC), is located on the first two floors of TUCC. It provides outpatient surgical treatment for a variety of urologic conditions including kidney stones and vasectomy reversals. All of the TUCC urologists perform procedures at USCC. Since January 2007, USCC has treated more than 29,000 patients, which equates to an average of 500 patients each month.[4]

23. In the ordinary course of receiving medical services and treatment from Defendant, patients are required to provide—and Plaintiffs did so provide—Defendant with extremely sensitive, personal and private information such as: (i) name, address, phone number and email address; (ii) date of birth; (iii) certain demographic information; (iv) Social Security number; (v) information relating to individual medical history; (vi) insurance information and coverage; (vii) information concerning an individual's doctor, nurse or other medical providers; (viii) photo identification; (ix) employer information, and (x) certain additional information deemed necessary to provide care.

[3] https://www.tucc.com/ (last visited Nov. 18, 2021).
[4] https://www.tucc.com/about-tucc/ (last visited Nov. 18, 2021).

24. Defendant also collects certain medical information about patients and creates records of the care it provides to them.

25. Additionally, Defendant 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, patients' health plan(s), close friends and/or family members.

Defendant Represented to Plaintiffs and Class Members That It Will Adequately Protect Their Private Information

26. TUCC recognizes its responsibility for the privacy of its patients' personal information and informs its patients that it is "strongly committed to maintaining your privacy."[5]

27. For example, Defendant has promulgated and adopted a notice of its privacy practices (the "Privacy Notice") with respect to how it handles patients' sensitive and confidential information.[6]

28. On information and belief, Defendant provides each of its patients, including Plaintiffs, with a Privacy Notice upon their first visit to TUCC.

29. Defendant's Privacy Notice is also accessible on its website.[7]

30. TUCC's Privacy Notice provides that PII will not be used or disclosed without written authorization.[8]

31. Defendant also notes in its Privacy Policy that it will only use or disclose PII without authorization as "permitted or required under law."[8]

---

[5] *Notice of Health Information Privacy Practices*, https://www.tucc.com/wp-content/uploads/2018/04/TUCCNotice-of-Privacy-Practices-2013.pdf (last visited Nov. 18, 2021).
[6] *Id.*
[7] *Id.*
[8] *Id.*

32. Defendant promises to maintain the confidentiality of patients' health, financial, and non-public personal information, ensure compliance with federal and state laws and regulations, and not to use or disclose patients' health information for any reasons other than those expressly listed in the Privacy Notice without written authorization.

33. As a condition of receiving medical care and treatment at Defendant's facilities, Defendant requires that its patients entrust it with highly sensitive personal information.

34. By obtaining, collecting, using, and deriving a benefit from Plaintiffs' and Class Members' Private Information, Defendant assumed legal and equitable duties and knew or should have known that it was responsible for protecting Plaintiffs' and Class Members' Private Information from unauthorized disclosure.

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

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

Defendant TUCC's "Data Security Incident"

37. According to its recent public statements, TUCC experienced a targeted cybersecurity incident between September 7, 2021 and September 8, 2021 when cyberthieves gained unauthorized access its network.[9]

38. Upon information and belief, the cyber attack was targeted at Defendant, due to its status as a healthcare entity that collects, creates and maintains both PII and PHI.

[9] *See Notice of Data Incident*, https://www.tucc.com/about-tucc/updates/ (last visited Nov. 18, 2021).

39. The targeted cyber-attack was expressly designed to gain access to private and confidential data, including, among other things, the PII and PHI of current and former patients like Plaintiffs and Class Members.

40. The Private Information contained in the files accessed by hackers was not encrypted.

41. The private information stolen from Defendant's system includes, but is not limited to, names, addresses, dates of birth, phone number, email address, Social Security Numbers (which are the keys to identity theft and financial fraud), medical record numbers, treating physicians, treating costs, diagnosis, and health insurance information.[10]

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

43. Plaintiffs and the 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.

44. By failing to protect the Private Information from cybercriminals, TUCC put all Class Members at risk of identity theft, financial fraud, and other serious harms.

45. Defendant negligently failed to take the necessary precautions required to safeguard and protect the Private Information of Plaintiffs and the other Class Members from unauthorized disclosure.

[10] *Id.*

46. Defendant's actions represent a flagrant disregard of Plaintiffs' and the other Class Members' rights.

47. Defendant hired a third-party security firm to perform an investigation into the full nature and scope of the Data Breach.

48. The investigation found that cybercriminals had been able to access patient data that included names, addresses, dates of birth, phone numbers, email addresses, Social Security Numbers, medical record numbers, treating physicians, treating costs, diagnosis, and health insurance information.[11]

49. At minimum, due to inadequate security precautions, between September 7, 2021 and September 8, 2021, the PII and PHI of 137,820 patients was exposed and compromised.

50. Plaintiffs received healthcare services at TUCC and provided certain PHI to Defendant during such treatment.

51. Plaintiffs received notice that their PHI and other private information was accessed and stolen by unauthorized third-party actors as a result of Defendant's failure to adequately protect its network.

The Cyber Attack that Compromised 137,820 Patients' PHI and Other Sensitive Information Was Entirely Foreseeable

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

[11] *Id.*

53. 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.

54. 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.

55. Data breaches, including those perpetrated against the healthcare sector of the economy, have become extremely widespread.

56. In 2019, a record 1,473 data breaches occurred, resulting in approximately 164,683,455 sensitive records being exposed, a 17% increase from 2018.[12]

57. Of the 1,473 recorded data breaches, 525 of them, or 35.64%, were in the medical or healthcare industry.[13]

58. Defendant was aware of the risk of data breaches because such breaches have dominated the headlines in recent years. For instance, the 525 reported breaches reported in 2019 exposed 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.[14]

59. In light of recent high profile cybersecurity incidents at other healthcare partner and provider companies, including, American Medical Collection Agency (25 million patients, March 2019) University of Washington Medicine (974,000 patients, December 2018), Florida Orthopedic Institute (640,000 patients, July 2020), Wolverine Solutions Group (600,000 patients, September

[12] *See 2019 End-Of-Year Data Breach Report*, Identity Theft Res. Ctr. (Jan. 8, 2020), https://www.idtheftcenter.org/wp-content/uploads/2020/01/01.28.2020_ITRC_2019-End-of-Year-Data-Breach-Report_FINAL_Highres-Appendix.pdf (last visited Nov. 18, 2021).
[13] *Id.*
[14] *Id.* at 15.

2018), Oregon Department of Human Services (645,000 patients, March 2019), Elite Emergency Physicians (550,000 patients, June 2020), Magellan Health (365,000 patients, April 2020), BJC Health System (286,876 patients, March 2020), Defendant knew or should have known that its electronic records would be targeted by cybercriminals.

60. In 2021 alone there have been over 220 data breach incidents. These approximately 220 data breach incidents have impacted nearly 15 million individuals.

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

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

63. 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."[15]

64. According to the 2019 Health Information Management Systems Society, Inc. ("HIMMS") Cybersecurity Survey, "[a] pattern of cybersecurity threats and experiences is discernable across U.S. healthcare organizations. Significant security incidents are a near-universal

[15] Ben Kochman, *FBI, Secret Service Warn Of Targeted Ransomware*, Law360 (Nov. 18, 2019, 9:44 PM), https://www.law360.com/consumerprotection/articles/1220974/fbi-secret-service-warn-of-targeted-ransomware?nl_pk=3ed44a08-fcc2-4b6c-89f0-aa0155a8bb51&utm_source=newsle tter&utm_medium=email&utm_campaign=consumerprotection (last visited Nov. 18, 2021).

experience in U.S. healthcare organizations with many of the incidents initiated by bad actors, leveraging emails as a means to compromise the integrity of their targets."[16]

65. Hospitals have emerged as a primary target because they sit on a gold mine of sensitive personally identifiable information for thousands of patients at any given time. From Social Security and insurance policies, to next of kin and credit cards, no other organization, including credit bureaus, have so much monetizable information stored in their data centers.[17]

66. PII and PHI is of great value to hackers and cybercriminals, and the data compromised in the Data Breach can be used in a variety of unlawful manners.

67. PII and PHI can be used to distinguish, identify or trace an individual's identity, such as their name, Social Security Number and medical records.

68. This can be accomplished alone or in combination with other personal or identifying information that is connected or linked to an individual, such as their birthdate, birthplace and mother's maiden name.

69. Given the nature of this Data Breach, it is foreseeable that the compromised PII and PHI can be used by hackers and cybercriminals in a variety of different ways.

70. Indeed, the cybercriminals who possess the Class Members' PII and PHI can readily obtain Class Members' tax returns or open fraudulent credit card accounts in the Class Members' names.

[16] *See* 2019 HIMSS Cybersecurity Survey (2019), https://www.himss.org/sites/hde/files/d7/u132196/2019_HIMSS_Cybersecurity_Survey_Final_Report.pdf (last visited Nov. 19, 2021).
[17] Eyal Benishti, *How to Safeguard Hospital Data from Email Spoofing Attacks*, Chief Healthcare Exec. (Apr. 4, 2019), https://www.chiefhealthcareexecutive.com/view/how-to-safeguard-hospital-data-from-email-spoofing-attacks (last visited Nov. 18, 2021).

71. 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, upon information and good faith belief, TUCC.

Defendant Fails to Comply with FTC Guidelines

72. 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.

73. 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 patient 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.

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

75. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect patient 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.

76. These FTC enforcement actions include actions against healthcare providers like Defendant. *See, e.g., In re 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.").

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

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

79. 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

80. 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.

81. 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.

82. 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.

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

84. These foregoing frameworks are existing and applicable industry standards in the healthcare industry, and Defendant failed to comply with these accepted standards, thereby opening the door to and causing the Data Breach.

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

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

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

87. Title II of HIPAA contains what are known as the Administrative Simplification provisions. These provisions require, among other things, that the Department of Health and Human Services ("HHS") create rules to streamline the standards for handling PHI and PII like the data Defendant left unguarded.

88. 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).

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

Defendant's Breach

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

91. 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' PHI and other 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).

92. As the result of allowing its computer systems to fall into dire need of security upgrading and its inadequate procedures for handling cybersecurity threats, Defendant negligently and unlawfully failed to safeguard Plaintiffs' and the Class Members' Private Information.

93. Accordingly, as outlined below, Plaintiffs and Class Members now face a substantial, increased, and immediate risk of fraud and identity theft. In addition, Plaintiffs and the Class Members also lost the benefit of the bargain they made with Defendant because of its inadequate data security practices for which they gave good and valuable consideration.

Data Breaches Cause Disruption & Put Consumers at Increased Risk of Fraud & Identity Theft

94. Hacking incidents and data breaches at medical facilities like Defendant's are especially problematic because of the disruption they cause to the medical treatment and overall daily lives of patients affected by the attack.

95. 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.[18]

96. Researchers have further found that at medical facilities that experienced a data security incident, the incident was associated with deterioration in timeliness and patient outcomes, generally.[19]

97. The United States Government Accountability Office released a report in 2007 regarding data breaches ("GAO Report") in which it noted that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."[20]

98. That is because any victim of a data breach is exposed to serious ramifications regardless of the nature of the data. Indeed, the reason criminals steal personally identifiable information is to monetize it. They do this by selling the spoils of their cyberattacks on the black market to identity thieves who desire to extort and harass victims, take over victims' identities in order to engage in illegal financial transactions under the victims' names. Because a person's identity is akin to a puzzle, the more accurate pieces of data an identity thief obtains about a person, the easier it is for the thief to take on the victim's identity, or otherwise harass or track the victim. For example, armed with just a name and date of birth, a data thief can utilize a hacking technique referred to as "social engineering" to obtain even more information about a victim's identity, such

[18] *See* Nsikan Akpan, *Ransomware and Data Breaches Linked to Uptick in Fatal Heart Attacks*, PBS (Oct. 24, 2019), https://www.pbs.org/newshour/science/ransomware-and-other-data-breaches-linked-to-uptick-in-fatal-heart-attacks (last visited Nov. 18, 2021).
[19] *See* Sung J. Choi et al., *Data Breach Remediation Efforts and Their Implications for Hospital Quality*, 54 Health Services Research 971, 971-980 (2019) https://onlinelibrary.wiley.com/doi/full/10.1111/1475-6773.13203 (last visited Nov. 18, 2021).
[20] *See* U.S. Gov. Accounting Office, GAO-07-737, *Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown* (2007), https://www.gao.gov/assets/gao-07-737.pdf (last visited Nov. 18, 2021).

as a person's login credentials or Social Security number. Social engineering is a form of hacking whereby a data thief uses previously acquired information to manipulate individuals into disclosing additional confidential or personal information through means such as spam phone calls and text messages or phishing emails.

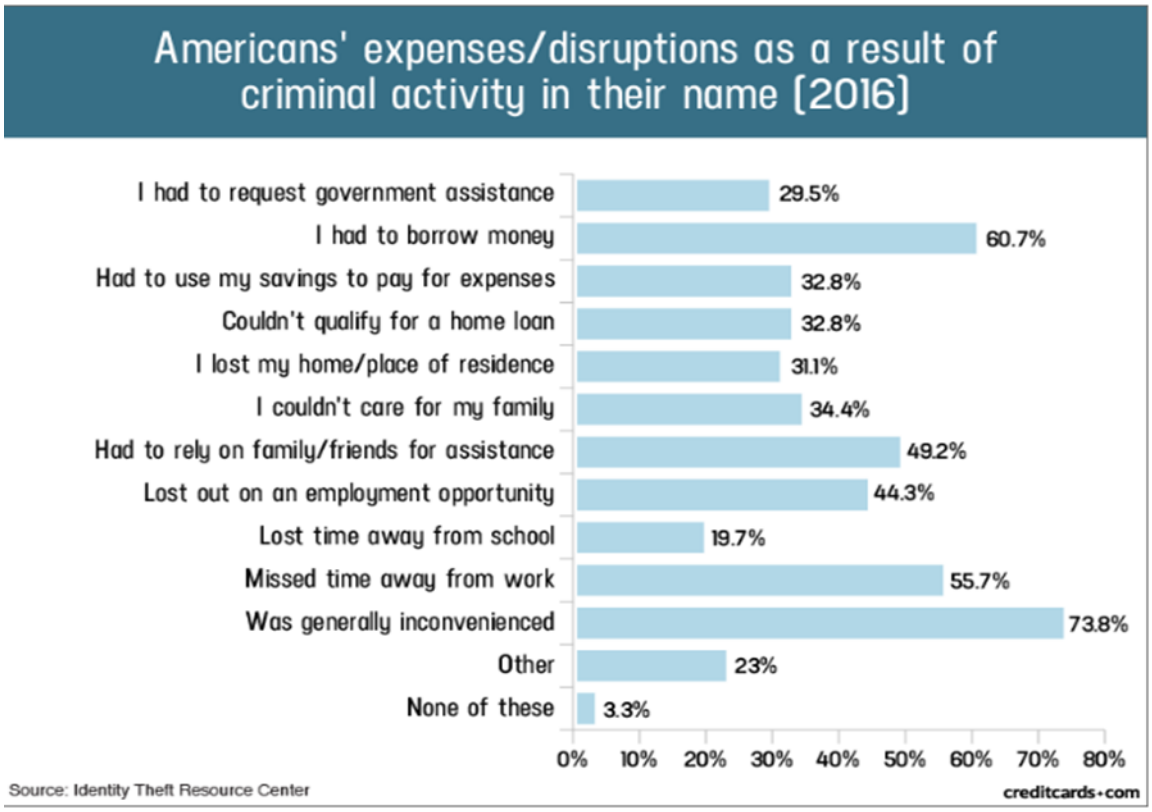
99. The FTC recommends that identity theft victims take several steps to protect their personal and financial information after a data breach, including contacting one of the credit bureaus to place a fraud alert (consider an extended fraud alert that lasts for 7 years if someone steals their identity), 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.[21]

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

101. 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.

[21] *See IdentityTheft.gov*, Federal Trade Commission, https://www.identitytheft.gov/#/Steps (last visited Nov. 18, 2021).

102. A study by Identity Theft Resource Center shows the multitude of harms caused by fraudulent use of personal and financial information:[22]



103. Moreover, theft of Private Information is also gravely serious. PII and PHI is an extremely valuable property right.[23]

104. Its value is axiomatic, considering the value of "big data" in corporate America and the fact that the consequences of cyber thefts include heavy prison sentences. Even this obvious

[22] *See* Jason Steele, *Credit Card and ID Theft Statistics*, CreditCards.com (Oct. 23, 2020), https://www.creditcards.com/credit-card-news/credit-card-security-id-theft-fraud-statistics-1276.php (last visited Nov. 18, 2021).

[23] *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). Available at: https://scholarship.richmond.edu/jolt/vol15/iss4/2 (last visited Nov. 18, 2021).

risk to reward analysis illustrates beyond doubt that Private Information has considerable market value.

105. 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."[24]

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

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

108. 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.

[24] *See* Federal Trade Commission, *What to Know About Medical Identity Theft*, http://www.consumer.ftc.gov/articles/0171-medical-identity-theft (last visited Nov. 18, 2021).

109. Private Information is such a valuable commodity to identity thieves that once the information has been compromised, criminals often trade the information on the "cyber black-market" for years.

110. 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.

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

112. Sensitive Private Information can sell for as much as $363 per record according to the Infosec Institute.[25] PII is particularly valuable because criminals can use it to target victims with frauds and scams. Once PII is stolen, fraudulent use of that information and damage to victims may continue for years.

113. For example, the Social Security Administration has warned that identity thieves can use an individual's Social Security number to apply for additional credit lines.[26] Such fraud may go undetected until debt collection calls commence months, or even years, later. Stolen Social Security numbers also make it possible for thieves to file fraudulent tax returns, file for unemployment benefits, or apply for a job using a false identity.[27] Each of these fraudulent activities is difficult to detect. An individual may not know that his or her Social Security number was used to file for unemployment benefits until law enforcement notifies the individual's

[25] *See* Ashiq Ja, *Hackers Selling Healthcare Data in the Black Market*, InfoSec (July 27, 2015), https://resources.infosecinstitute.com/topic/hackers-selling-healthcare-data-in-the-black-market/ (last visited Nov. 18, 2021).
[26] *Identity Theft and Your Social Security Number* at 1, Soc. Sec. Admin. (2018), https://www.ssa.gov/pubs/EN-05-10064.pdf (last visited Nov. 18, 2021).
[27] *Id.* at 4.

employer of the suspected fraud. Fraudulent tax returns are typically discovered only when an individual's authentic tax return is rejected.

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

115. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. Even then, a new Social Security number may not be effective, as "[t]he credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[28]

116. Medical information is especially valuable to identity thieves.

117. According to account monitoring company LogDog, medical data sells for $50 and up on the Dark Web.[29]

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

119. For this reason, Defendant knew or should have known about these dangers and strengthened its network and data security 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.

[28] Brian Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR (Feb. 9, 2015), http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millions-worrying-about-identity-theft (lasty visited Nov. 18, 2021).

[29] Lisa Vaas, *Ransomware Attacks Paralyze, and Sometimes Crush, Hospitals*, Naked Security (Oct. 3, 2019), https://nakedsecurity.sophos.com/2019/10/03/ransomware-attacks-paralyze-and-sometimes-crush-hospitals/#content (last visited Nov. 18, 2021).

Plaintiffs' and Class Members' Damages

120. To date, Defendant has done less than nothing to adequately protect Plaintiffs and Class Members' identities, or to compensate them for their injuries sustained in this data breach. Defendant's data breach notice letter completely downplays and disavows the theft of Plaintiffs and Class Members Private Information, when the facts demonstrate that the Private Information was accessed and exfiltrated. The complimentary fraud and identity monitoring service offered by Defendant is wholly inadequate as the services are only offered for 12 months and it places the burden squarely on Plaintiffs and Class Members by requiring them to expend time signing up for that service, as opposed to automatically enrolling all victims of this cybercrime.

121. Plaintiffs and Class Members have been injured and damaged by the Data Breach.

122. Plaintiff Snyder is a patient of Defendant.

123. Plaintiff Snyder typically takes measures to protect her Private Information, and is very careful about sharing her PII and PHI. She has never knowingly transmitted unencrypted PII or PHI over the internet or any other unsecured source.

124. Plaintiff Snyder stores any documents containing her PII and PHI in a safe and secure location. Moreover, she diligently chooses unique usernames and passwords for her online accounts.

125. To the best of her knowledge, Plaintiff Snyders's Private Information was never compromised in any other data breach.

126. Plaintiff Diona Lopez was a patient of TUCC several times before the Data Breach event. In or about October of 2021, Plaintiff Lopez received a notification letter from Defendant stating that her PII was taken, which included her "date of birth, Social Security number, address,

phone number, email address, medical record number, diagnosis, treating physician, insurance provider, treatment cost, and/or guarantor name."

127. The letter also offered one or two years of credit monitoring through IDX, which was and continues to be ineffective for Lopez and the other class members. The IDX credit monitoring would have shared Ms. Lopez's information with third parties and could not guarantee complete privacy of her sensitive PII.

128. In the months and years following the Data Breach, Ms. Lopez and the other class members will experience a slew of harms as a result of Defendant's ineffective data security measures. Some of these harms will include fraudulent charges, medical procedures ordered in patients' names without their permission, and targeted advertising without patient consent.

129. Plaintiff Lopez greatly values her privacy, especially in receiving medical services, and would not have paid the amount that she did for services at TUCC if she had known that her information would be maintained using inadequate data security systems.

130. Although Ms. Lopez is mitigating the harm done to her and her family as a result of the exposure of his Private Information, she is still unsure of the extent that he has been harmed because Defendant is unable to notify her of exactly what type of Private Information was compromised in the Security Breach.

131. 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.

132. As a direct and proximate result of Defendant's conduct, Plaintiffs and Class Members have been forced to expend time dealing with the effects of the Data Breach. The notice letter itself provided her with a list of steps to take to protect her information. For example, Plaintiff

Snyder has been forced to spend time replacing monitoring her financial accounts for unauthorized activity.

133. As a direct and proximate result of Defendant's conduct, Plaintiff Snyder has experienced a significant increase in spam phone calls, all of which appear to have been placed with the intent to commit identity theft by way of a social engineering attack.

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

135. 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.

136. Plaintiffs and Class Members may also incur out-of-pocket costs for protective measures such as credit monitoring fees (for any credit monitoring obtained in addition to or in lieu of the inadequate monitoring offered by Defendant), credit report fees, credit freeze fees, and similar costs directly or indirectly related to the Data Breach.

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

138. Plaintiffs and Class Members were also damaged via benefit-of-the-bargain damages. Plaintiffs and Class Members overpaid for a service that was intended to be accompanied by adequate data security but was not. Part of the price Plaintiffs and Class Members paid to Defendant was intended to be used by Defendant to fund adequate security of SJ/C's computer

property and protect Plaintiffs' and Class Members' Private Information. Thus, Plaintiffs and the Class Members did not get what they paid for.

139. 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. Indeed, Defendant's own notice of data breach provides instructions to Plaintiffs and Class Members about all the time that they will need to spend monitor their own accounts and statements received from healthcare providers and health insurance plans.

140. Plaintiffs and Class Members have suffered actual injury as a direct result of the Data Breach. Many victims suffered ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach relating to:

- Finding fraudulent loans, insurance claims, tax returns, and/or government benefit claims;
- Purchasing credit monitoring and identity theft prevention;
- Placing "freezes" and "alerts" with credit reporting agencies;
- Spending time on the phone with or at a financial institution or government agency to dispute fraudulent charges and/or claims;
- Contacting financial institutions and closing or modifying financial accounts; and
- Closely reviewing and monitoring Social Security number, medical insurance accounts, bank accounts, and credit reports for unauthorized activity for years to come.

141. 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 sensitive and confidential personal, health, and/or financial information is not accessible online, that access to such data is password-protected, and that such data is properly encrypted.

142. Further, as a result of Defendant's conduct, Plaintiffs and Class Members are forced to live with the anxiety that their Private Information may be disclosed to the entire world, thereby subjecting them to embarrassment and depriving them of any right to privacy whatsoever.

143. As a direct and proximate result of Defendant's actions and inactions, Plaintiffs and Class Members have suffered a loss of privacy and are at a substantial and present risk of harm.

CLASS ACTION ALLEGATIONS

144. Plaintiffs bring this action on behalf of themselves and on behalf of all other persons similarly situated ("the Class") pursuant to Colo. R. P. 23.

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

> **National Class:** All persons whose PII and/or PHI was compromised as a result of the Data Breach (the "National Class" or the "Class").
>
> **Colorado Sub-Class:** All persons in Colorado whose PII and/or PHI was compromised as a result of the Data Breach (the "Colorado Sub-Class" and together with the National Class, the "Classes").

146. Excluded from the Classes 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 Classes are Members of the judiciary to whom this case is assigned, their families and Members of their staff.

147. Certification of Plaintiffs' claims for class-wide treatment is appropriate because Plaintiffs can prove the elements of their 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.

148. **Numerosity**. The Members of the Class are so numerous that joinder of all of them is impracticable. Based on Defendant's report to HHS OCR, the Class members consists of approximately 137,820 current and former patients of TUCC whose data was compromised in the Data Breach.[30]

149. **Commonality and Predominance.** There are questions of law and fact common to the Classes, 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' PII;

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

c. Whether Defendant's data security systems prior to and during the Data Breach complied with applicable data security laws and regulations;

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

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

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

[30] https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf.

g. Whether computer hackers obtained Class Members' PII in the Data Breach;

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 violated the Colorado Consumer Protection Act; and

k. Whether Defendant violated Colorado's data security laws;

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

150. Defendant engaged in a common course of conduct giving rise to the legal rights Plaintiffs seek to enforce, on behalf of herself and the other members of the Classes, 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. Similar or identical statutory and common law violations, business practices, and injuries are involved. Individual questions, if any, pale in comparison, in both quality and quantity, to the numerous common questions that dominate this action. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

151. **Adequacy of Representation**. Plaintiffs will fairly and adequately represent and protect the interests of the Members of the Classes. Their interests do not conflict with the interests of other members of the Classes they seek to represent. They have retained competent and experienced counsel, and they will prosecute this action vigorously. Plaintiffs' Counsel are

competent and experienced in litigating complex class actions, including data privacy litigation of this kind.

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

153. All members of the proposed Classes are readily ascertainable. TUCC has access to current and former patient names and addresses affected by the Data Breach. Using this information, Class Members can be identified and ascertained for the purpose of providing notice.

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

CAUSES OF ACTION

FIRST COUNT

NEGLIGENCE
(On Behalf of Plaintiffs & All Class Members)

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

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

157. The Class Members are individuals who provided certain PII and PHI to Defendant TUCC including their names, addresses, dates of birth, diagnosis codes, Social Security numbers, CPT codes and treatment dates as a necessary condition of TUCC providing medical services to the Class Members.

158. TUCC had full knowledge of the sensitivity of the PII and PHI to which it was entrusted and the types of harm that Class Members could and would suffer if the PII and PHI were wrongfully disclosed.

159. TUCC had a duty to each Class Member to exercise reasonable care in holding, safeguarding and protecting that information.

160. Plaintiffs and the Class Members were the foreseeable victims of any inadequate safety and security practices.

161. The Class Members had no ability to protect their data in TUCC's possession.

162. By collecting and storing this data in its computer property, and by 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 the Class Members' Private Information held within it—to prevent disclosure of the information and to safeguard the information from theft.

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

164. Defendant owed a duty of care to Plaintiffs and the 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.

165. 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 the common law.

166. 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.

167. 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).

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

169. 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.

170. 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.

171. Defendant breached its duties, and thus was negligent, by failing to use reasonable measures to protect the Class Members' Private Information.

172. The specific negligent acts and omissions committed by Defendant TUCC include, but are not limited to, the following:

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

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

c. Failure to periodically ensure that their network 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;

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

g. Failing to have mitigation and back-up plans in place in the event of a cyber-attack and data breach.

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

174. Further, the breach of security was reasonably foreseeable given the known high frequency of cyber-attacks and data breaches in the medical industry.

175. 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.

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

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

SECOND COUNT

BREACH OF IMPLIED CONTRACT
(On Behalf of Plaintiffs and All Class Members)

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

179. 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 Plaintiff's and Class Members' Private Information.

180. Specifically, Plaintiffs and the Class Members entered into a valid and enforceable implied contracts with Defendant when they first went for medical treatment at one of Defendant's facilities.

181. The valid and enforceable implied contracts to provide medical healthcare services that Plaintiffs and Class Members entered into with Defendant included Defendant's promise to protect nonpublic Private Information given to Defendant or that Defendant created on its own from Plaintiffs' and the Class Members' disclosures.

182. Plaintiffs and Class Members provided this Private Information in reliance of that promise.

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

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

185. 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.

186. Plaintiffs and 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.

187. Under the implied 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.

188. In exchange, Plaintiffs and Members of the Class agreed to pay money for these services, and to turn over their Private Information.

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

190. The implied contracts for the provision of medical services—contracts that include the contractual obligations to maintain the privacy of Plaintiffs' and the Class Members' Private Information—are also acknowledged, memorialized, and embodied in multiple documents, including (among other documents) Defendant's Privacy Policy and Notice of Privacy Practices.

191. Defendant's express representations, including, but not limited to the express representations found in its Privacy Policy and Notice of Privacy Practices, memorialize and embody an implied contractual obligation requiring Defendant to implement data security adequate to safeguard and protect the privacy of Plaintiffs and Class Members' Private Information.

192. Consumers of healthcare value their privacy, the privacy of their dependents, and the ability to keep their Private Information associated with obtaining healthcare private.

193. To customers such as Plaintiffs and the 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.

194. Plaintiffs and Class Members would not have entrusted their Private Information to Defendant and entered into these implied contracts with Defendant without an understanding that their Private Information would be safeguarded and protected or 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.

195. A meeting of the minds occurred when Plaintiffs and the Class Members 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, (a) the provision of healthcare and medical services and (b) the protection of their Private Information.

196. Plaintiffs and the Class Members performed their obligations under the contract when they paid for their healthcare services and provided their Private Information.

197. 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 Data Breach.

198. Defendant materially breached the terms of its implied contracts, including, but not limited to, the terms stated in the relevant Privacy Policy and Notice of Privacy Practices.

199. Defendant did not maintain the privacy of Plaintiffs' and the Class Members' Private Information as evidenced by its late notification of the Data Breach to Plaintiff and approximately 137,820 Class Members.

200. Specifically, Defendant did not comply with industry standards, the 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.

201. The Data Breach was a reasonably foreseeable consequence of Defendant's actions in breach of these contracts.

202. As a result of Defendant's failure to fulfill the data security protections promised in these contracts, Plaintiffs and Class Members did not receive the full benefit of their bargains, and instead received healthcare and other services that were of a diminished value compared to that described in the contracts.

203. 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.

204. 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 provided their sensitive data in exchange for healthcare services.

205. As a direct and proximate result of the Data Breach, Plaintiffs and the 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.

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

207. Plaintiffs and the 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.

THIRD COUNT

BREACH OF FIDUCIARY DUTY
(On Behalf of Plaintiffs and All Class Members)

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

209. 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.

210. Defendant TUCC accepted the special confidence placed in it by Plaintiffs and

Class Members, as evidenced by its assertion that it is "respects the needs of clients for confidentiality, privacy, and security" and by the promulgation of its Privacy Notice. There was an understanding between the parties that Defendant would act for the benefit of Plaintiffs and Class Members in preserving the confidentiality of the Private Information.

211. In light of the special relationship between Defendant, Plaintiffs, and the Class Members, whereby Defendant became the guardian of Plaintiffs' and the Class Members' Private Information, Defendant accepted a fiduciary duty to act primarily for the benefit of its patients, including Plaintiffs and the Class Members. This duty included safeguarding Plaintiffs' and the Class Members' Private Information.

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

213. Defendant breached its fiduciary duties to Plaintiffs and Class Members by failing to diligently discovery, investigate, or give notice of the Cyber-Attack and Data Breach in a reasonable and practicable period of time.

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

215. Defendant breached the fiduciary duties it owed to Plaintiffs and the Class Members by failing to timely notify and/or warn them of the Cyber-Attack and Data Breach.

216. Defendant breached its fiduciary duties 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).

217. Defendant breached its fiduciary duties 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).

218. Defendant breached its fiduciary duties 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).

219. Defendant breached its fiduciary duties 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).

220. Defendant breached its fiduciary duties 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).

221. Defendant breached its fiduciary duties 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).

222. Defendant breached its fiduciary duties 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).

223. Defendant breached its fiduciary duties 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.

224. Defendant breached its fiduciary duties by failing to effectively train all members

of its workforce (including independent contractors) on the policies and procedures necessary to maintain the security of PHI, in violation of 45 C.F.R. § 164.530(b) and 45 C.F.R. § 164.308(a)(5).

225. Defendant breached its fiduciary duties by failing to design, implement, and enforce policies and procedures establishing physical and administrative safeguards to reasonably safeguard PHI, in violation of 45 C.F.R. § 164.530(c).

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

227. 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 Cyber-Attack and data breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (v) the continued risk to their Private Information, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information in its continued possession; (vi) future costs in terms of time, effort, and money that will be expended as result of the Cyber-Attack and data breach for the remainder of the lives of Plaintiffs and Class Members; and (vii) the diminished value of Defendant's services they received.

228. As a direct and proximate result of Defendant's breaches of its fiduciary duties, Plaintiffs and the Class Members have suffered and will continue to suffer other forms of injury

and/or harm, and other economic and non-economic losses.

FOURTH COUNT

VIOLATION OF COLORADO'S DATA SECURITY LAWS, COLO. REV. STAT. 6-1-713.5
(On Behalf of Plaintiffs and Colorado Subclass Members)

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

230. Plaintiffs bring this claim on behalf of themselves and the Class.

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

232. Colo. Rev. Stat. § 6-1-713.5 requires commercial entities who maintain, own, or license "personal identifying information of an individual residing in the state" to "implement and maintain reasonable security procedures and practices that are appropriate to the nature of the personal identifying information and the nature and size of the business and its operations."

233. Defendant's conduct violated Colo. Rev. Stat. § 6-1-713.5. Specifically, Defendant voluntarily undertook the act of maintaining and storing Plaintiffs' PII and PHI but Defendant failed to implement safety and security procedures and practices sufficient enough to protect from the data breach that it should have anticipated. Defendant should have known and anticipated that data breaches—especially health data—were on the rise, and that medical institutions were lucrative or likely targets of cybercriminals looking to steal PII. Correspondingly, Defendant should have implemented and maintained procedures and practices appropriate to the nature and scope of information compromised in the data breach.

234. As a result of Defendant's violation of Colo. Rev. Stat. § 6-1-716, Plaintiffs and the Class Members incurred economic damages, including expenses associated with necessary credit

monitoring.

235. Accordingly, Plaintiffs, individually and on behalf of the Class, respectfully request this Court award all relevant damages.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, individually and on behalf of the Classes defined herein, prays for judgment as against Defendant TUCC 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' PII, 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 compromised during the Data Breach;

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

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

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

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

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

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

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

JURY TRIAL DEMANDED

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

Dated: April 27, 2022 Respectfully submitted,

/s/ Rick D. Bailey
Rick D. Bailey, Esq. (CO Bar No. 26554)
LAW OFFICE OF RICK D. BAILEY, ESQ.
1085 Lafayette St., Ste 702
Denver, Colorado 80218
Phone: (720) 676-6023
rick@rickbaileylaw.com

David K. Lietz (pro hac vice motion filed and pending)
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN, PLLC
5335 Wisconsin Avenue NW
Suite 440
Washington, D.C. 20015-2052
Telephone: (866) 252-0878
Facsimile: (202) 686-2877
Email: dlietz@milberg.com

Nicholas A. Migliaccio (pro hac vice forthcoming)
Jason Rathod (pro hac vice forthcoming)
Kevin Leddy (pro hac vice forthcoming)
Migliaccio & Rathod, LLP
412 H Street NE

Washington, D.C. 20002
202.470.3520
nmigliaccio@classlawdc.com

Attorneys for Plaintiffs & the Proposed Classes