IN THE IOWA DISTRICT COURT FOR JOHNSON COUNTY

MICHAEL CLARK, individually and on behalf of all others similarly situated, Plaintiffs, v. MERCY HOSPITAL, IOWA CITY, IOWA, d/b/a Mercy Iowa City, Defendant.	Case No. _____ **PETITION AT LAW and JURY TRIAL DEMAND**

CLASS ACTION PETITION

Plaintiff MICHAEL CLARK ("Plaintiff"), individually and on behalf of all others similarly situated, brings this action against Defendant MERCY HOSPITAL, IOWA CITY, IOWA ("Mercy" or "Defendant"), an Iowa non-profit corporation that does business as "Mercy Iowa City," to obtain damages, restitution, and injunctive relief for the Class, as defined below, from Defendant. Plaintiff makes the following allegations upon information and belief, except as to his own actions, the investigation of his counsel, and the facts that are a matter of public record:

NATURE OF THE ACTION

1. This class action arises out of the recent targeted cyberattack and data breach ("Data Breach") at Mercy, a health-care provider and hospital that offers clinical care services throughout southeastern Iowa. As a result of the Data Breach, Plaintiff and approximately 92,795 Class Members, 86,910 of whom are residents of Iowa, suffered ascertainable losses in the form of the loss of the benefit of their bargain, out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the attack.

2. In addition, Plaintiff's and Class Members' sensitive personal information—which was entrusted to Defendant—was compromised and unlawfully accessed due to the Data Breach.

3. Information compromised in the Data Breach includes patient names, dates of birth, Social Security numbers, driver's license numbers, health insurance information and medical treatment information and other protected health information as defined by the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), and additional personally identifiable information ("PII") and protected health information ("PHI") that Defendant collected and maintained (collectively the "Private Information").

4. Plaintiff brings this class action lawsuit to address Defendant's inadequate safeguarding of Class Members' Private Information that it collected and maintained, and for failing to provide timely and adequate notice to Plaintiff and Class Members that their information had been subject to the unauthorized access of an unknown third party and precisely what specific type of information was accessed.

5. Defendant maintained the Private Information in a reckless manner.

6. In particular, the Private Information was maintained on Defendant's computer network in a condition vulnerable to cyberattacks, such as the phishing attack that obtained Defendant's employees' credentials and access to Defendant's network.

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

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

property, it would have discovered the intrusion sooner.

9. Plaintiff's and Class Members' identities are now at risk because of Defendant's negligent 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' names to obtain medical services, using Class Members' health information to target other phishing and hacking intrusions based on their individual health needs, using Class Members' information to obtain government benefits, filing fraudulent tax returns using Class Members' information, obtaining driver's licenses in Class Members' names but with another person's photograph, and giving false information to police during an arrest.

11. As a result of the Data Breach, Plaintiff and Class Members have been exposed to a heightened and imminent risk of fraud and identity theft. Plaintiff and Class Members must now and in the future closely monitor their financial accounts to guard against identity theft.

12. Plaintiff 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. Plaintiff seeks to remedy these harms on behalf of himself and all similarly situated individuals whose Private Information was accessed during the Data Breach.

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

Defendant.

PARTIES

15. Plaintiff Michael Clark is, and at all times mentioned herein was, an individual citizen of the State of Iowa residing in the City of Mount Pleasant. Plaintiff has been receiving heath care services as a patient from Mercy since 2013. Plaintiff most recently received medical services or treatments from Mercy in June 2020. Plaintiff was notified of Defendant's Data Breach and his Private Information being compromised upon receiving a letter titled "Notification of a Data Security Incident" sent by Defendant.[1]

16. Defendant Mercy is a healthcare services provider with its principal place of business at 500 East Market Street, Iowa City, Iowa 52245.

JURISDICTION AND VENUE

17. The Court has subject matter jurisdiction over Plaintiff's claims under Iowa Code § 602.6101.

18. Venue is proper in Johnson County pursuant to Iowa Code § 616.17 and § 616.18 because Defendant Mercy is headquartered and does business in this County, the cause of action accrued in this county, and Mercy has an office for the transaction of its customary business in this county.

19. The Court has personal jurisdiction over Defendant because Defendant is an Iowa non-profit corporation with its principal place of business in Iowa, committed tortious acts in Iowa, and because Defendant has sufficient minimum contacts and engaged in significant business activity in the State of Iowa.

[1] *See* Exhibit A.

DEFENDANT'S BUSINESS

20. Defendant Mercy is an acute care hospital, healthcare services provider, and regional referral center offering its services and treatments throughout southeast Iowa.[2]

21. Mercy provides care in many major medical specialties including primary care, bariatrics, cardiology, maternity care, oncology, ear/nose/throat, emergency medicine and care, ophthalmology, pulmonology, sleep medicine, anesthesia, general surgery, orthopedics, urology, gastroenterology, neurology, podiatry, radiology, pediatrics, and others.[3]

22. In addition, Defendant provides home healthcare, hospice, rehabilitation, and lab services,[4] as well as operating and managing centers and clinics for cancer, weight loss, neurodiagnostic sleep, nutrition, wound care and veins, internal medicine, primary care, behavioral health, and occupational health.[5]

23. Mercy's hospital facility consists of 234 acute care beds, 25 rooms for outpatient surgery, and a 23-bed nursery.[6]

24. Defendant Mercy maintains a "medical staff comprised of more than 250 doctors"[7] as well as approximately 1,100 other employees, which as of 2018 made Mercy the fourth largest employer in Iowa City.[8]

25. In 2019, Mercy reported revenues of approximately $516 million.[9]

---

[2] *About Mercy*, Mercy Iowa City, http://www.mercyiowacity.org/about-mercy (last visited Jan. 12, 2021).
[3] *See Medical Services*, Mercy Iowa City, http://www.mercyiowacity.org/medical-services (last visited Jan. 13, 2021).
[4] *Id*.
[5] *See Mercy Iowa City Clinics*, Mercy Iowa City, http://www.mercyiowacity.org/mercy-clinics (last visited Jan. 13, 2021).
[6] Supra, note 2.
[7] *Id*.
[8] City of Iowa City Financial Dept., Comprehensive Annual Financial Report, City of Iowa City, 137 (June 30, 2018), https://www8.iowa-city.org/weblink/0/edoc/1836591/FY2018%20CAFR.pdf.
[9] *Iowa Hospital 2019 – 2017 Total Facility Financial Data – Urban Hospitals*, Iowa Hospital Association, 23 (last visited Jan. 13, 2021), http://www.iowahospitalfacts.com/Documents/Iowa_Hospital_Data.pdf.

26. In 2017, Defendant Mercy became an affiliate of the MercyOne healthcare network, formerly known as the Mercy Health Network.[10] MercyOne is "a connected system of healthcare facilities and services" that maintains 420 health care locations, employs over 20,000 people, and generates over $3 billion in revenue.[11]

27. In the ordinary course of receiving treatment and health care services from Mercy, patients are required to provide sensitive personal and private information such as:

- Names;
- Dates of birth;
- Social Security numbers;
- Driver's license numbers;
- Tribal identification numbers;
- Financial account information;
- Payment card information;
- Medical histories;
- Treatment information;
- Medication or prescription information;
- Beneficiary information;
- Provider information;
- Address, phone number, and email address, and;

[10] *See Mercy Announces New Affiliation*, Mercy Iowa City (April 28, 2017), https://www.mercyiowacity.org/news/?id=21&sid=1&nid=148.
[11] *Fact Sheet*, MercyOne, https://www.mercyone.org/desmoines/_assets/documents/portals/mercyonefactsheet2020a.pdf (last visited Jan. 13, 2021).

- Health insurance information.

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

29. On information and belief, Mercy provides each of its patients with a HIPAA compliant notice of its privacy practices (the "Privacy Notice") in respect to how they handle patients' sensitive and confidential information.[12]

30. Due to the highly sensitive and personal nature of the information Mercy acquires and stores with respect to its patients, Mercy promises in its Privacy Notice and throughout its website, to, among other things, maintain the privacy of patients' health information.

31. On Mercy's Patient Rights and Responsibilities webpage, Defendant states that it "Respects the patient's right to personal privacy, including confidentiality of his or her clinical records."[13]

32. In its Patient Guide, Defendant asserts to its patients that "You can expect us to [p]rotect your privacy and the confidentiality of your health information."[14] Moreover, in the Personal Privacy and Security section of Defendant's Patient Guide, Defendant declares that "Mercy Iowa City is dedicated to protecting your privacy. Personal information about a diagnosis or treatment must come from your health care provider and is only shared with people you choose."[15]

---

[12] *See Your Privacy*, Mercy Iowa City, http://www.mercyiowacity.org/HIPAA (last visited Jan. 13, 2021).
[13] *Patient Rights and Responsibilities*, Mercy Iowa City, http://www.mercyiowacity.org/patient-rights-and-responsibilities (last visited Jan. 13, 2021).
[14] *Mercy Iowa City Patient Guide*, Mercy Iowa City, 3 (last visited Jan. 13, 2021), http://www.mercyiowacity.org/upload/docs/Patients%20and%20Visitors/New%20%20Patient%20Guide%20Contents%20NEWa.pdf.
[15] *Id* at 13.

33. Defendant's Privacy Notice, titled *Notice Regarding Compliance By Mercy Iowa City With Health Insurance Portability and Accountability Act Privacy, Security, and Other Regulations*, provides, in relevant part, the following:

> Your Privacy Is Important To Us
>
> At Mercy Iowa City, we are committed to providing our patients with Exceptional Medicine, Extraordinary Care. **An important part of our commitment is our pledge to protect your non-public personal medical and financial information.** This notice, which is required by the federal Health Insurance Portability and Accountability Act of 1996 (HIPAA), informs you about our privacy practices[.]
>
> Pursuant to the Health Insurance Portability and Accountability Act of 1996 (HIPAA), U.S. Department of Health and Human Services (HHS) is promulgating regulations that address, among other things; 1) standards for the privacy of individually identifiable health information; 2) security standards to protect the confidentiality and integrity of health information and the information technology used to store, process, and transmit such data; and 3) standards for administrative transactions and data elements exchanged electronically that are consistent with the goals of improving the operation of the health care system and reducing administrative costs.
>
> Please note that HHS has released some final regulations, with varying dates for compliance, and some proposed, but not final, regulations. After HHS has issued final HIPAA regulations, **Mercy Iowa City will undertake a review to its policies, practices, and standards to [e]nsure compliance with all applicable regulations.**
>
> Our Privacy Pledge
>
> **Mercy Iowa City does not disclose your non-public personal medical and financial information, except as required or permitted by law.** Mercy Iowa City does not sell patient information. We do not disclose this information, even when our patient relationships end, except as required or permitted by law.
>
> **Mercy Iowa City will ensure that its practices and standards comply with HIPAA and other applicable federal and state laws**

> **and regulations.** Mercy Iowa City will work with appropriate regulatory and accreditation agencies to ensure consistency between Mercy Iowa City's policies and HIPAA. Consistent with Mercy Iowa City's policy on statutory variances, **Mercy Iowa City will uphold the higher privacy standard when there is a conflict between applicable state and federal regulations. In the event the privacy of your personal medical or financial information is compromised, Mercy Iowa City will notify you of any known breach to your unsecured information.**[16]

(emphasis added).

34. Thus, as disclosed in its Privacy Notice, Mercy promises to maintain the confidentiality of patients' health, financial, and non-public personal information, ensure compliance with federal and state laws and regulations, and to notify patients of any breach that jeopardizes their private information.[17]

35. 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.

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

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

38. Plaintiff 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.

---

[16] *Your Privacy*, Mercy Iowa City, http://www.mercyiowacity.org/HIPAA (last visited Jan. 13, 2021).
[17] *Id*.

THE CYBERATTACK AND DATA BREACH

39. On or around June 24, 2020, Mercy became aware that an "employee's email account had been used to send out spam/phishing emails[.]"[18]

40. Mercy launched an investigation into this suspicious activity and determined that due to the phishing scheme, an unauthorized third party gained access to one Mercy employee's email account.[19]

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

42. Upon information and belief, the targeted phishing cyberattack was expressly designed to gain access to private and confidential data, including (among other things) the PII and PHI of patients like Plaintiff and the Class Members.

43. Because of this targeted phishing attack, data thieves were able to gain access to an employee email account and subsequently access the protected Private Information of many Mercy patients.

44. Further, Mercy's investigation also uncovered that the unauthorized intrusion and access occurred for more than a month between May 15, 2020 and June 24, 2020.[20]

45. The email account and messages contained therein affected by this incident contained some combination of the following information: patient names, social security numbers, driver's license numbers, dates of birth, medical treatment information, and health insurance information.[21]

---

[18] See https://www.iowaattorneygeneral.gov/media/cms/11132020_Mercy_Iowa_City_1D095956B076E.pdf (last visited Jan 14, 2021).
[19] *Id.*
[20] *Id.*
[21] *Id.*

46. The Private Information contained in the emails was not encrypted.

47. Plaintiff's Private Information was accessed and stolen in the Data Breach. Plaintiff further believes his stolen Private Information was subsequently sold on the Dark Web.

48. Unsurprisingly, Mercy could not rule out that Private Information was viewed or accessed in the Data Breach.[22]

49. Mercy informed impacted customers that they should take steps to "protect themselves against fraudulent activity and identity theft" and to remain vigilant about unauthorized access to their accounts.[23]

50. Further, though Mercy claims that they "hold [them]selves accountable for the human, financial, and natural resources entrusted to [their] care[,]"[24] Defendant is only offering a complimentary twelve month membership of identity monitoring services through Experian for victim patients whose social security number or driver's license number was compromised.[25]

51. The offer of identity monitoring services is an acknowledgment by Mercy that the impacted customers are subject to an imminent threat of fraud and identity theft.

52. Despite discovering the Data Breach on or about June 24, 2020, and acknowledging that data thieves likely accessed Plaintiff's and the Class Members' Private Information, Mercy did not begin to notify affected patients until November 13, 2020, nearly four and a half months later.[26]

53. Moreover, some impacted patients, approximately 26,437 victims from Iowa, did not receive their notice of the Data Breach until November 30, 2020, over five months after the

[22] *Id*.
[23] *Id.*
[24] *Mission and Values*, Mercy Iowa City, http://www.mercyiowacity.org/mission-values (last visited Jan. 14, 2021).
[25] *Supra*, note 18.
[26] *Id*.

breach was discovered.[27]

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

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

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

57. In light of recent high profile data breaches at other healthcare partner and provider companies, including, American Medical Collection Agency (25 million patients, March 2019) University of Washington Medicine (974,000 patients, December 2018), Florida Orthopedic Institute (640,000 patients, July 2020), Wolverine Solutions Group (600,000 patients, September 2018), Oregon Department of Human Services (645,000 patients, March 2019), Elite Emergency Physicians (550,000 patients, June 2020), Magellan Health (365,000 patients, April 2020), BJC Health System (286,876 patients, March 2020), Mercy knew or should have known that its electronic records would be targeted by cybercriminals

58. Indeed, cyberattacks have become so notorious that the Federal Bureau of Investigation 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

[27] See https://www.iowaattorneygeneral.gov/media/cms/11302020_Mercy_Iowa_City__Supplemen_D5BB893E16DBA.pdf (last visited Jan. 14, 2021).

municipalities and hospitals are attractive. . . because they often have lesser IT defenses and a high incentive to regain access to their data quickly."[28]

59. In fact, according to the cybersecurity firm Mimecast, "90% of healthcare organizations experienced email-borne attacks in the past year[.]"[29]

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

61. Phishing attacks of the type that the unauthorized persons used to gain access to Defendant's employee email accounts are among the oldest, most common, and well-known form of cyberattacks.

62. According to Verizon, over 90% of all cybersecurity attacks that result in a data breach start with a phishing attack.[30]

63. "Phishing is a cyber-attack that uses disguised email as a weapon. The goal is to trick the email recipient into believing that the message is something they want or need — a request from their bank, for instance, or a note from someone in their company — and to click a link or download an attachment."[31] The fake link will typically mimic a familiar website and require the input of credentials. Once inputted, the credentials are then used to gain unauthorized access into a system. "It's one of the oldest types of cyber-attacks, dating back to the 1990s" and one that every organization with an internet presence is aware.[32] It remains the "simplest kind of

---

[28] *FBI, Secret Service Warn of Targeted*, Law360 (Nov. 18, 2019), https://www.law360.com/articles/1220974/fbi-secret-service-warn-of-targeted-ransomware (last visited Jan. 13, 2021).
[29] *See* Maria Henriquez, Iowa City Hospital Suffers Phishing Attack, Security Magazine (Nov. 23, 2020), https://www.securitymagazine.com/articles/93988-iowa-city-hospital-suffers-phishing-attack.
[30] *Verizon Says Phishing Drives 90% of Cybersecurity Breaches*, Graphus (Jan. 21, 2020), https://www.graphus.ai/verizon-says-phishing-still-drives-90-of-cybersecurity-breaches/.
[31] Josh Fruhlinger, *What is Phishing? How This Cyber-Attack Works and How to Prevent It*, CSO Online (Sept. 4, 2020), https://www.csoonline.com/article/2117843/what-is-phishing-how-this-cyber-attack-works-and-how-to-prevent-it.html.
[32] *Id.*

cyberattack and, at the same time, the most dangerous and effective."[33]

64. Phishing attacks are generally preventable with the implementation of a variety of proactive measures such as purchasing and using some sort of commonly available anti-malware security software (such as the ubiquitous Malwarebites). Most cybersecurity tools have the ability to detect when a link or an attachment is not what it seems.[34]

65. Other proactive measures include sandboxing inbound e-mail (*i.e.*, an automated process that segregates e-mail with attachments and links to an isolated test environment, or a "sandbox," wherein a suspicious file or URL may be executed safely), multi-factor authentication, inspecting and analyzing web traffic, penetration testing (which can be used to test an organization's security policy, its adherence to compliance requirements, its employees' security awareness and the organization's ability to identify and respond to security incidents), and employee education, just to name some of the well-known tools and techniques to prevent phishing attacks.

Defendant Fails to Comply with FTC Guidelines

66. 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.

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

[33] *What is Phishing?*, Malwarebytes, https://www.malwarebytes.com/phishing/ (last visited Jan. 14, 2021).
[34] *Id.*

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.[35] 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.[36]

68. 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.

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

70. These FTC enforcement actions include actions against healthcare providers like Defendant. *See, e.g., In the Matter of Labmd, Inc., A Corp*, 2016-2 Trade Cas. (CCH) ¶ 79708, 2016 WL 4128215, at *32 (MSNET July 28, 2016) ("[T]he Commission concludes that LabMD's

[35] *Protecting Personal Information: A Guide for Business*, Federal Trade Commission (2016). Available at https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last visited Jan. 14, 2021).
[36] *Id*.

data security practices were unreasonable and constitute an unfair act or practice in violation of Section 5 of the FTC Act.")

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

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

73. 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

74. 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.

75. 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.

76. A number of industry and national best practices have been published and should be used as a go-to resource when developing an institution's cybersecurity standards.

77. The Center for Internet Security (CIS) released its *Critical Security Controls*, and all healthcare institutions are strongly advised to follow these actions. The CIS Benchmarks are the overwhelming option of choice for auditors worldwide when advising organizations on the

adoption of a secure build standard for any governance and security initiative, including PCI DSS, HIPAA, NIST 800-53, SOX, FISMA, ISO/IEC 27002, Graham Leach Bliley and ITIL.[37]

78. 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.

79. Defendant failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework, NIST Special Publications 800-53, 53A, or 800-171; General Accounting Office (GAO) standards; the Federal Risk and Authorization Management Program (FEDRAMP); and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

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

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

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

82. Title II of HIPAA contains what are known as the Administrative Simplification provisions. 42 U.S.C. §§ 1301, *et seq*. These provisions require, among other things, that the Department of Health and Human Services ("HHS") create rules to streamline the standards for

[37] *See CIS Benchmarks FAQ*, Center for Internet Security, https://www.cisecurity.org/cis-benchmarks/cis-benchmarks-faq/ (last visited Jan. 14, 2021).

handling PII like the data Mercy left unguarded. The HHS subsequently promulgated multiple regulations under authority of the Administrative Simplification provisions of HIPAA. These rules include 45 C.F.R. § 164.306(a)(1-4); 45 C.F.R. § 164.312(a)(1); 45 C.F.R. § 164.308(a)(1)(i); 45 C.F.R. § 164.308(a)(1)(ii)(D), and 45 C.F.R. § 164.530(b).

83. Phishing attacks are also considered a breach under the HIPAA Rules because there is an access of PHI not permitted under the HIPAA Privacy Rule:

> A breach under the HIPAA Rules is defined as, "...the acquisition, access, use, or disclosure of PHI in a manner not permitted under the [HIPAA Privacy Rule] which compromises the security or privacy of the PHI." *See* 45 C.F.R. 164.40

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

DEFENDANT'S BREACH

85. Mercy breached its obligations to Plaintiff and Class Members and/or was otherwise negligent and reckless because it failed to properly maintain and safeguard its computer systems and data. Mercy's unlawful conduct includes, but is not limited to, the following acts and/or omissions:

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

b. Failing to adequately protect patients' Private Information;

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

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

e. Failing to train its employees in the proper handling of emails containing PII and PHI;

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

g. Failing to implement technical policies and procedures for electronic information systems that maintain electronic PHI to allow access only to those persons or software programs that have been granted access rights in violation of 45 C.F.R. § 164.312(a)(1);

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

i. Failing to implement procedures to review records of information system activity regularly, such as audit logs, access reports, and security incident tracking reports in violation of 45 C.F.R. § 164.308(a)(1)(ii)(D);

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

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

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

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

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

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

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

p. Failing to adhere to industry standards for cybersecurity.

86. As the result of computer systems in dire need of security upgrading, inadequate procedures for handling emails containing viruses or other malignant computer code, and employees who opened files containing the virus or malignant code that perpetrated the cyberattack, Mercy negligently and unlawfully failed to safeguard Plaintiff's and Class Members' Private Information.

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

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

88. Cyberattacks and data breaches at medical facilities like Mercy are especially problematic because of the disruption they cause to the overall daily lives of patients affected by

the attack.

89. The United States Government Accountability Office released a report in 2007 regarding data breaches ("GAO Report") in which it noted that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."[38]

90. 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 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.

91. 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

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

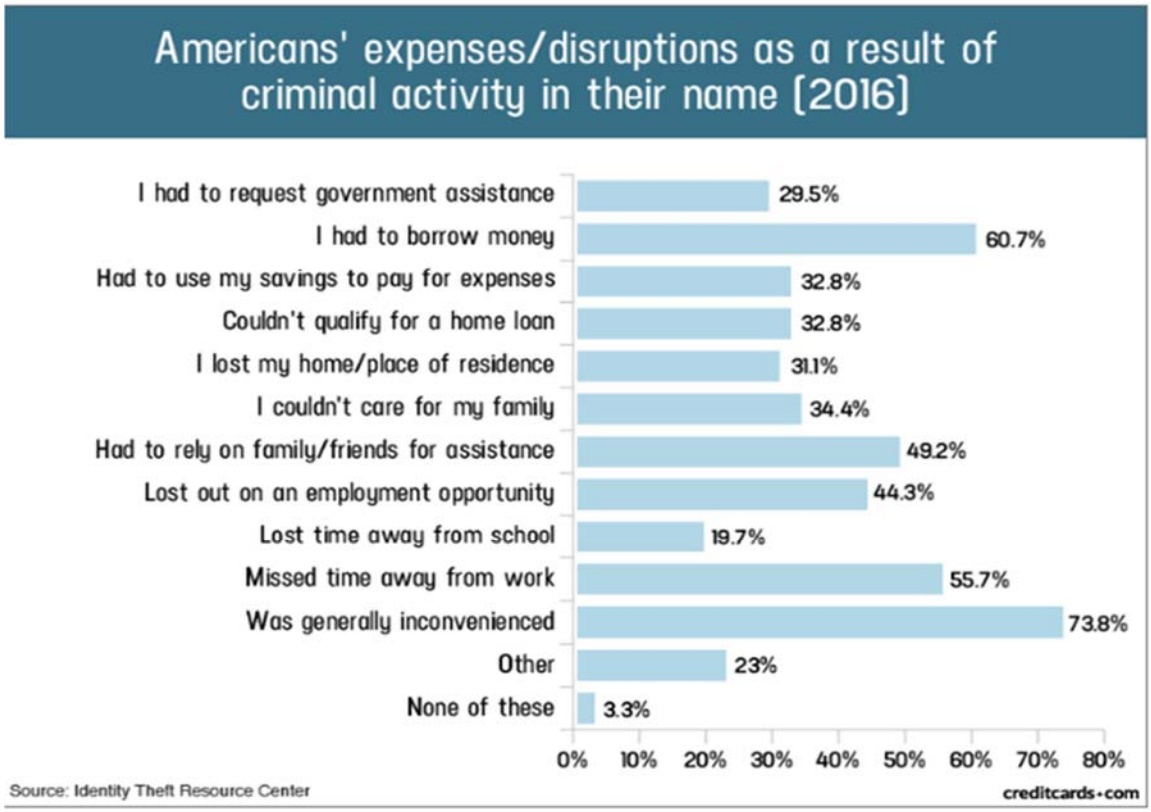
charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.[39]

92. 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.

93. 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.

94. A study by Identity Theft Resource Center shows the multitude of harms caused by fraudulent use of personal and financial information:[40]

[39] *See IdentityTheft.gov*, Federal Trade Commission, https://www.identitytheft.gov/Steps (last visited January 13, 2021).
[40] *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.



95. Moreover, theft of Private Information is also gravely serious. PII and PHI is an extremely valuable property right.[41]

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

97. 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,

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

insurance and payment records, and credit report may be affected."[42]

98. 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.

99. 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.

100. 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.

101. 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.

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

---

[42] *See* Federal Trade Commission, *Medical Identity Theft*, http://www.consumer.ftc.gov/articles/0171-medical-identity-theft (last visited Jan. 13, 2021).

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

104. Sensitive Private Information can sell for as much as $363 per record according to the Infosec Institute.[43] 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.

105. 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.[44] 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.[45] Each of these fraudulent activities is difficult to detect. An individual may not know that his or her Social Security Number was used to file for unemployment benefits until law enforcement notifies the individual's employer of the suspected fraud. Fraudulent tax returns are typically discovered only when an individual's authentic tax return is rejected.

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

107. 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

[43] *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/.
[44] *Identity Theft and Your Social Security Number*, Social Security Administration (2018) at 1. Available at https://www.ssa.gov/pubs/EN-05-10064.pdf (last visited Jan. 14, 2021).
[45] *Id* at 4.

number."[46]

108. This data, as one would expect, demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "[c]ompared to credit card information, personally identifiable information and Social Security Numbers are worth more than 10x on the black market."[47]

109. Medical information is especially valuable to identity thieves.

110. According to account monitoring company LogDog, coveted Social Security numbers were selling on the dark web for just $1 in 2016 – the same as a Facebook account.[48] That pales in comparison with the asking price for medical data, which was selling for $50 and up.[49]

111. 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.

112. For this reason, Mercy knew or should have known about these dangers and strengthened its data and email handling systems accordingly. Mercy 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.

Plaintiff's and Class Members' Damages

113. To date, Defendant has done absolutely nothing to provide Plaintiff and Class

[46] 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.

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

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

[49] 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.

Members with relief for the damages they have suffered as a result of the Data Breach.

114. The complimentary fraud and identity monitoring service offered by Mercy is wholly inadequate as the services are only offered for 12 months and it places the burden squarely on Plaintiff and Class Members by requiring them to expend time signing up for that service, as opposed to automatically enrolling all victims of this cybercrime.

115. Further, Defendant is only offering the complimentary monitoring service to patients whose social security number and/or driver's license number was compromised. This is utterly unacceptable as it leaves numerous victims of the breach, who do not fall into that category, vulnerable to all sorts of fraud and identity theft.

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

117. After the Data Breach occurred, Plaintiff Clark experienced numerous fraudulent and unauthorized charges to his Mastercard account. Between May 2020 and December 2020, Plaintiff discovered the following unauthorized and fraudulent charges on his account:[50]

a) A charge of $18.95 from PublicCardCheck.com on May 23, 2020;

b) A charge of $1.00 from PublicCardCheck.com on May 26, 2020;

c) A charge of $18.95 from PublicCardCheck.com on June 21, 2020;

d) A charge of $18.95 from PublicCardCheck.com on July 21, 2020;

e) A charge of $18.95 from PublicCardCheck.com on August 20, 2020;

f) A charge of $18.95 from PublicCardCheck.com on September 19, 2020;

g) A charge of $18.95 from PublicCardCheck.com on October 19, 2020;

h) A charge of $5.00 from Skype.com on October 28, 2020;

[50] *See* Exhibit B.

i) A charge of $5.00 from Skype.com on October 31, 2020;

j) A charge of $18.95 from PublicCardCheck.com on November 18, 2020; and,

k) A charge of $15.98 from ProBiller.com on December 3, 2020;

118. Plaintiff has never heard of or purchased services from either PublicCardCheck.com or ProBiller.com. Moreover, Plaintiff does not have a Skype account.

119. Upon discovering the aforementioned fraudulent charges, Plaintiff filed a fraud claim with his bank and was subsequently reimbursed $143.65.[51]

120. Plaintiff has expended a great deal of time and effort dealing with these fraudulent charges and the numerous other possible ramifications as a result of Defendant's Data Breach.

121. Plaintiff's PII and PHI was compromised as a direct and proximate result of the Data Breach.

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

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

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

125. Plaintiff 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

[51] *Id.*

fraudsters could use that information to more effectively target such schemes to Plaintiff and Class Members.

126. Plaintiff and Class Members may also incur out-of-pocket costs for protective measures such as credit monitoring fees, credit report fees, credit freeze fees, and similar costs directly or indirectly related to the Data Breach.

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

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

129. Plaintiff 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 Plaintiff and Class Members about all the time that they will need to spend monitor their own accounts, or to establish a "security freeze" on their credit report.[52]

130. Plaintiff and Class Members have suffered or will suffer actual injury as a direct result of the Data Breach. Many victims suffered ascertainable losses in the form of out-of-pocket

[52] *See Notice of Data Security Event*, Mercy (Dec. 16, 2020), https://oag.ca.gov/system/files/Attachment%20-%20CA%20Individual%20Notice%20Letters.pdf.

expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach relating to:

a. Finding fraudulent charges, insurance claims, and/or government benefit claims;

b. Purchasing credit monitoring and identity theft prevention;

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

d. Spending time on the phone with or at a financial institution or government agency to dispute fraudulent charges and/or claims;

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

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

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

132. Further, as a result of Mercy's conduct, Plaintiff and Class Members are forced to live with the anxiety that their Private Information—which contains the most intimate details about a person's life, including what ailments they suffer, whether physical or mental—may be disclosed to the entire world, thereby subjecting them to embarrassment and depriving them of any right to privacy whatsoever.

133. As a direct and proximate result of Mercy's actions and inactions, Plaintiff and

Class Members have suffered a loss of privacy and are at an imminent and increased risk of future harm.

CLASS REPRESENTATION ALLEGATIONS

134. Pursuant to Iowa Rule of Civil Procedure 1.262, Plaintiff seeks certification of the following classes of persons defined as follows:

> **National Class:** All persons Mercy identified as being among those individuals impacted by the Data Breach, including all who were sent a notice of the Data Breach.
>
> **Iowa Sub-Class:** All persons residing in the State of Iowa that Mercy identified as being among those individuals impacted by the Data Breach, including all who were sent a notice of the Data Breach.

Excluded from the Classes are any judges presiding over this matter and court personnel assigned to this case.

135. **Numerosity**: The Class Members are so numerous that joinder of all members is impracticable. Though the exact number and identities of Class Members are unknown at this time, the Classes reportedly include approximately 92,795 people. The identities of Class Members are ascertainable through Mercy's records, Class Members' records, publication notice, self-identification, and other means.

136. **Commonality**. 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 Mercy unlawfully used, maintained, lost, or disclosed Plaintiff's and Class Members' Private Information;

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

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

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

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

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

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

i. Whether Mercy owed a duty to provide Plaintiff and Class Members notice of this Data Breach, and whether Defendant breached that duty to provide timely notice;

j. Whether Plaintiff and Class Members suffered legally cognizable damages as a result of Mercy's misconduct;

k. Whether Mercy's conduct was negligent;

l. Whether Mercy's conduct violated federal law;

m. Whether Mercy's conduct violated state law;

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

137. Common sources of evidence may also be used to demonstrate Mercy's unlawful conduct on a class-wide basis, including, but not limited to, documents and testimony about its data and cybersecurity measures (or lack thereof); testing and other methods that can prove Mercy's data and cybersecurity systems have been or remain inadequate; documents and testimony about the source, cause, and extent of the Data Breach; and documents and testimony about any remedial efforts undertaken as a result of the Data Breach.

138. **Typicality**. Plaintiff's claims are typical of the claims of the respective Class he seeks to represent, in that the named Plaintiff and all members of the proposed Class have suffered similar injuries as a result of the same practices alleged herein. Plaintiff has no interests adverse to the interests of the other members of the Class.

139. **Adequacy of Representation**. Plaintiff will fairly and adequately represent and protect the interests of the Members of the Class. Plaintiff's Counsel is competent and experienced in litigating Class actions, including data privacy litigation of this kind.

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

141. **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 Mercy. 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.

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

143. Certification is appropriate because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

a. Whether Mercy owed a legal duty to Plaintiff and the Classes to exercise due care in collecting, storing, and safeguarding their Private Information;

b. Whether Mercy's security measures to protect their data systems were reasonable in light of best practices recommended by data security experts;

c. Whether Mercy's failure to institute adequate protective security measures amounted to negligence;

d. Whether Mercy failed to take commercially reasonable steps to safeguard consumer Private Information; and

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

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

CLAIMS FOR RELIEF

COUNT I
NEGLIGENCE
(On Behalf of Plaintiff and the Classes)

145. Plaintiff repeats and re-alleges each and every factual allegation contained in paragraphs 1-144 as if fully set forth herein. Plaintiff brings this claim individually and on behalf of the Class Members.

146. In order to receive medical treatments and services, Mercy and/or its agents required Plaintiff and Class Members to submit non-public Private Information, such as PII and PHI.

147. Plaintiff and Class Members entrusted their Private Information to Mercy and/or its Agents with the understanding that Mercy would safeguard their information.

148. By collecting and storing this data in its computer property, and sharing it and using it for commercial gain, Defendant had a duty of care to use reasonable means to secure and safeguard its computer property—and Class Members' Private Information held within it—to prevent disclosure of the information, and to safeguard the information from theft. Defendant's duty included a responsibility to implement processes by which 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.

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

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

151. 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).

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

153. 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.

154. 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.

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

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

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

c. Failure to periodically ensure that their network system had plans in place to maintain reasonable data security safeguards;

d. Failing to adequately train its employees to recognize and contain phishing attacks;

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

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

g. Failing to timely notify Class Members about the Cyber-Attack regarding what type of Private Information had been compromised so that they could take appropriate steps to mitigate the potential for identity theft and other damages; and

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

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

157. 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.

158. Plaintiff and Class Members are entitled to compensatory and consequential damages suffered as a result of the Cyber-Attack and data breach.

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

COUNT II
BREACH OF IMPLIED CONTRACT
(On Behalf of Plaintiff and the Classes)

160. Plaintiff re-alleges and incorporates by reference all paragraphs as if fully set forth herein.

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

162. Specifically, Plaintiff entered into a valid and enforceable implied contract with Defendant when he first went for medical care and treatment at one of Defendant's facilities.

163. The valid and enforceable implied contracts to provide medical health care services that Plaintiff and Class Members entered into with Defendant and/or its agents include the promise to protect non-public Private Information given to Defendant or that Defendant creates on its own from disclosure.

164. When Plaintiff and Class Members provided their Private Information to Defendant

and/or its agents in exchange for medical services, they entered into implied contracts with Defendant pursuant to which Defendant agreed to reasonably protect such information.

165. Defendant and/or its agents solicited and invited Class Members to provide their Private Information as part of Defendant's regular business practices. Plaintiff and Class Members accepted Defendant's offers and provided their Private Information to Defendant.

166. In entering into such implied contracts, Plaintiff 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.

167. 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.

168. Under the implied contracts, Defendant and/or its agents promised and were obligated to: (a) provide healthcare to Plaintiff and Class Members; and (b) protect Plaintiff's and the Class Members' PII/PHI: (i) provided to obtain such health care; and/or (ii) created as a result of providing such health care. In exchange, Plaintiff and Members of the Class agreed to pay money for these services, and to turn over their Private Information.

169. Both the provision of medical services healthcare and the protection of Plaintiff's and Class Members' Private Information were material aspects of these implied contracts.

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

171. Defendant's express representations, including, but not limited to the express

representations found in its Privacy Notice, memorializes and embodies the implied contractual obligation requiring Defendant to implement data security adequate to safeguard and protect the privacy of Plaintiff's and Class Members' Private Information.

172. Consumers of healthcare value their privacy, the privacy of their dependents, and the ability to keep their Private Information associated with obtaining healthcare private. To customers such as Plaintiff and Class Members, healthcare that does not adhere to industry standard data security protocols to protect Private Information is fundamentally less useful and less valuable than healthcare that adheres to industry-standard data security. Plaintiff and Class Members would not have entrusted their Private Information to Defendant and/or its Agents 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.

173. A meeting of the minds occurred, as Plaintiff and Members of the Class agreed to and did provide their Private Information to Defendant and/or its agents, and paid for the provided healthcare in exchange for, amongst other things, both the provision of health care and medical services and the protection of their Private Information.

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

175. Defendant materially breached its contractual obligation to protect the non-public Private Information Defendant gathered when the sensitive information was accessed by unauthorized personnel as part of the Cyber-Attack and Data Breach.

176. Defendant materially breached the terms of the implied contracts, including, but

not limited to, the terms stated in the relevant Privacy Notice. Defendant did not maintain the privacy of Plaintiff's and Class Members' Private Information as evidenced by its notifications of the Data Breach to Plaintiff and approximately 92,795 Class Members. Specifically, Defendant did not comply with industry standards, standards of conduct embodied in statutes like HIPAA and Section 5 of the FTCA, or otherwise protect Plaintiff's and the Class Members' Private Information, as set forth above.

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

178. As a result of Defendant's failure to fulfill the data security protections promised in these contracts, Plaintiff and Members of the Class did not receive the full benefit of the bargain, and instead received health care and other medical services that were of a diminished value to that described in the contracts. Plaintiff 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 health care they received.

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

180. As a direct and proximate result of the Data Breach, Plaintiff and Class Members have been harmed and have suffered, and will continue to suffer, actual damages and injuries, including without limitation the release and disclosure of their Private Information, the loss of control of their Private Information, the imminent risk of suffering additional damages in the future, disruption of their medical care and treatment, out-of-pocket expenses, and the loss of the

benefit of the bargain they had struck with Defendant.

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

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

COUNT III
UNJUST ENRICHMENT
(On Behalf of Plaintiff and the Classes)

183. Plaintiff re-alleges and incorporates by reference all paragraphs as if fully set forth herein.

184. This count is plead in the alternative to the breach of contract counts above.

185. Plaintiff and Class Members conferred a monetary benefit on Defendant. Specifically, they purchased goods and services from Defendant and/or its agents and in so doing provided Defendant with their Private Information. In exchange, Plaintiff and Class Members should have received from Defendant the goods and services that were the subject of the transaction and have their Private Information protected with adequate data security.

186. Defendant knew that Plaintiff and Class Members conferred a benefit which Defendant accepted. Defendant profited from these transactions and used the Private Information of Plaintiff and Class Members for business purposes.

187. The amount Plaintiff and Class Members paid for goods and services were used, in part, to pay for use of Defendant's network and the administrative costs of data management and security.

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

189. Defendant failed to secure Plaintiff's and Class Members' Private Information and, therefore, did not provide full compensation for the benefit Plaintiff and Class Members provided.

190. Defendant acquired the Private Information through inequitable means in that it failed to disclose the inadequate security practices previously alleged.

191. If Plaintiff and Class Members knew that Defendant had not reasonably secured their Private Information, they would not have agreed to Defendant's services.

192. Plaintiff and Class Members have no adequate remedy at law.

193. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have suffered and will suffer injury, including but not limited to: (a) actual identity theft; (b) the loss of the opportunity of how their Private Information is used; (c) the compromise, publication, and/or theft of their Private Information; (d) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, and/or unauthorized use of their Private Information; (e) lost opportunity costs associated with efforts expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (f) 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 Private Information in their continued possession; and (g) future costs in terms of time, effort, and money that will be expended

to prevent, detect, contest, and repair the impact of the Private Information compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and Class Members.

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

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

COUNT IV
BREACH OF CONFIDENCE
(On Behalf of Plaintiff and the Classes)

196. Plaintiff re-alleges and incorporates by reference all paragraphs as if fully set forth herein.

197. At all times during Plaintiff's and Class Members' interactions with Defendant and/or its agents, Defendant was fully aware of the confidential and sensitive nature of Plaintiff's and Class Members' Private Information.

198. As alleged herein and above, Defendant's relationship with Plaintiff and Class Members was governed by terms and expectations that Plaintiff's and Class Members' Private Information would be collected, stored, and protected in confidence, and would not be disclosed to unauthorized third parties.

199. Plaintiff and Class Members provided their Private Information to Defendant and/or its agents with the explicit and implicit understandings that Defendant would protect and not permit the Private Information to be disseminated to any unauthorized parties.

200. Plaintiff and Class Members also provided their Private Information to

Defendant and/or its agents with the explicit and implicit understandings that Defendant would take precautions to protect such Private Information from unauthorized disclosure.

201. Defendant voluntarily received in confidence Plaintiff's and Class Members' Private Information with the understanding that the Private Information would not be disclosed or disseminated to the public or any unauthorized third parties.

202. Due to Defendant's failure to prevent, detect, or avoid the Data Breach from occurring by, inter alia, following industry standard information security practices to secure Plaintiff's and Class Members' Private Information, Plaintiff's and Class Members' Private Information was disclosed and misappropriated to unauthorized third parties beyond Plaintiff's and Class Members' confidence, and without their express permission.

203. As a direct and proximate cause of Defendant's actions and/or omissions, Plaintiff and Class Members have suffered damages.

204. But for Defendant's disclosure of Plaintiff's and Class Members' Private Information in violation of the parties' understanding of confidence, their protected Private Information would not have been compromised, stolen, viewed, accessed, and used by unauthorized third parties. Defendant's Data Breach was the direct and legal cause of the theft of Plaintiff's and Class Members' protected Private Information, as well as the resulting damages.

205. The injury and harm Plaintiff and Class Members suffered was the reasonably foreseeable result of Defendant's unauthorized disclosure of Plaintiff' and Class Members' Private Information.

206. As a direct and proximate result of Defendant's breach of confidence, Plaintiff 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, tax fraud, and/or unauthorized use of their Private Information; (iv) lost opportunity costs associated with effort expended to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from medical fraud, financial fraud and identity theft; (v) costs associated with placing freezes on credit reports; (vii) the continued risk to their Private Information, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information of patients in their continued possession; and (viii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the Private Information compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and Class Members.

207. As a direct and proximate result of Defendant's breach of confidence, Plaintiff and Class Members have suffered and will continue to suffer injury and/or harm.

COUNT V
VIOLATION OF THE IOWA CONSUMER FRAUD ACT ("ICFA")
IOWA CODE §§ 714H.3, 714h.5.
(On Behalf of Plaintiff and the National Class, or Alternatively the Iowa Sub-Class)

208. Plaintiff re-alleges and incorporates by reference all paragraphs as if fully set forth herein.

209. ICFA prohibits a person or entity from:

> [Engaging] in a practice or act the person knows or reasonably should know is an unfair practice, deception, fraud, false pretense, or false promise, or the misrepresentation, concealment, suppression, or omission of a material fact, with the intent that

> others rely upon the unfair practice, deception, fraud, false pretense, false promise, misrepresentation, concealment, suppression, or omission in connection with the advertisement [and/or] sale[.]

Iowa Code § 714H.3(1).

210. Iowa Code defines an unfair practice as "an act or practice which causes substantial, unavoidable injury to consumer that is not outweighed by any consumer or competitive benefits which the practice produces." Iowa Code § 714.16(1)(n).

211. Defendant engaged in the conduct alleged in this Complaint through transactions in and involving trade and commerce.

212. While involved in trade or commerce, Defendant violated the ICFA, by engaging in unfair, deceptive, and unconscionable business practices including, among other things, by:

a. Failing to implement and maintain appropriate and reasonable security procedures and practices to safeguard and protect the Private Information of Defendant's client patients from unauthorized access and disclosure;
b. Failing to disclose the material fact that its computer systems and data security practices were inadequate to safeguard and protect the Private Information of Defendant's client patients from being compromised, stolen, lost, or misused; and
c. Failing to disclose the Data Breach to Defendant's client patients in "the most expeditious manner possible and without unreasonable delay" in violation of Iowa Code § 715C.2(1).

213. Defendant knew or should have known that the Mercy computer systems and data security practices were inadequate to safeguard Class Members' Private Information entrusted to

it, and that risk of a data breach or theft was highly likely.

214. Defendant should have disclosed this information because Defendant was in a superior position to know the true facts related to the defective data security.

215. Defendant's failures constitute an unfair practice and false, deceptive, and misleading representations regarding the security of Mercy's network and aggregation of Private Information.

216. These unfair practices and misleading representations upon which impacted individuals (including Plaintiff and Class Members) relied were material facts (e.g., as to Defendant's adequate protection of Private Information), and consumers (including Plaintiff and Class Members) relied on those representations to their detriment.

217. In committing the acts alleged above, Defendant engaged in fraudulent, deceptive, and unfair practices by omitting, failing to disclose, or inadequately disclosing to Defendant's client patients that it did not follow industry best practices for the collection, use, and storage of Private Information.

218. As a direct and proximate result of Defendant's conduct, Plaintiff and other Members of the Class have been harmed and have suffered damages including, but not limited to: damages arising from attempted identity theft and fraud; out-of-pocket expenses associated with procuring identity protection and restoration services; increased risk of future identity theft and fraud, and the costs associated therewith; and time spent monitoring, addressing and correcting the current and future consequences of the Data Breach.

219. As a direct and proximate result of Defendant's fraudulent, deceptive, and unfair practices and omissions, Plaintiff's and Class Members' Private Information was disclosed to third parties without authorization, causing and will continue to cause Plaintiff and Class Members

damages. Accordingly, Plaintiff and Class Members are entitled to recover actual damages, an order providing declaratory and injunctive relief, and reasonable attorneys' fees and costs, to the extent permitted by law.

COUNT VI
VIOLATION OF THE IOWA PERSONAL INFORMATION SECURITY BREACH PROTECTION ACT ("PISBPA")
IOWA CODE § 715C.2
(On Behalf of Plaintiff and the National Class, or Alternatively the Iowa Sub-Class)

220. Plaintiff re-alleges and incorporates by reference all paragraphs as if fully set forth herein.

221. PISBPA states that:

> Any person who owns or licenses computerized data that includes a consumer's personal information that is used in the course of the person's business…and that was subject to a breach of security shall give notice of the breach of security following discovery of such breach of security…to any consumer whose personal information was included in the information that was breached. The consumer notification shall be made in the most expeditious manner possible and without unreasonable delay[.]

Iowa Code § 715C.2(1).

222. Defendant Mercy is a business that licenses computerized data, which includes personal information, of Plaintiff and Members of the Class.

223. As defined by Iowa Code § 715C.1(11)(a)(1-3), "personal information" is defined as "an individual's first name or first initial and last name in combination with any one or more of the following[:] social security number, driver's license number, and financial account

information.

224. Defendant Mercy acted as a licensee of the sensitive Private Information in using it to identify patients, file claims, provide medical services, and by storing this valuable and highly sensitive information on its computer systems and network.

225. Defendant became aware of the intrusion and Data Breach on June 24, 2020, yet shockingly it only began to send out notice to victims of the breach on November 13, 2020, approximately four and a half months later.

226. Per Iowa Code § 715C.2(2), Defendant was required to send notice of the breach to victims "immediately following discovery of such breach of security if a consumer's personal information was included[.] Though Plaintiff's and Class Member's personal information was included in the breach and compromised, Defendant failed to send the requisite "immediate" notice under Iowa law.

227. Because Defendant was aware of the breach of security of its systems, Defendant had an obligation to disclose the Data Breach in a timely fashion without unreasonable delay.

228. In failing to timely disclose the Data Breach, Plaintiff and the Class Members were harmed because they were not able to immediately take precautionary action to prevent and mitigate the effects of identity theft and financial fraud.

229. By failing to disclose the Data Breach in a timely and reasonable manner, Defendant violated Iowa Code §§ 715C.2(1).

230. Pursuant to Iowa Code § 715C.2(9), a violation of this section is considered an unlawful practice under Iowa Code §§ 714.16(7).

231. As a direct and proximate result of Defendant's violation of the notice requirement under PISBPA, Plaintiff and Class Members suffered the above-mentioned damages. Accordingly,

Plaintiff and Class Members are entitled to recover actual damages, injunctive relief, and reasonable attorneys' fees and costs, to the extent permitted by law.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on his own and behalf of all others similarly situated, prays for relief as follows:

A. For an Order certifying this case as a class action pursuant to Iowa Rule of Civil Procedure 1.262, appointing Plaintiff as Class Representatives, and the undersigned as Class Counsel;

B. Awarding monetary, punitive and actual damages and/or restitution, as appropriate;

C. Awarding declaratory and injunctive relief as permitted by law or equity to assure that the Class has an effective remedy, including enjoining Mercy from continuing the unlawful practices as set forth above;

D. Prejudgment interest to the extent allowed by the law;

E. Awarding all costs, experts' fees and attorneys' fees, expenses and costs of prosecuting this action; and

F. Such other and further relief as the Court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiff hereby demands a trial by jury of all claims so triable.

DATED: January 19, 2021

Respectfully submitted,

Gary E. Mason*
David K. Lietz*
MASON LIETZ & KLINGER LLP
5301 Wisconsin Avenue, NW
Suite 305
Washington, DC 20016
Tel: (202) 429-2290
gmason@masonllp.com
dlietz@masonllp.com

Gary M. Klinger*
MASON LIETZ & KLINGER LLP
227 W. Monroe Street, Suite 2100
Chicago, IL 60606
Tel: (202) 429-2290
gklinger@masonllp.com

Syed Ali Saeed*
SAEED & LITTLE, LLP
18 E. Vermont Street
Indianapolis, IN 46204
317.721.9214 (t)
888.422.3151 (f)
ali@sllawfirm.com

Brad Schroeder
HARTUNG SCHROEDER LAW FIRM
303 Locust Street, Ste. 300
Des Moines, Iowa 50309
515-282-7800 (t)
515-282-8700 (f)
Schroeder@hartungschroeder.com

**pro hac vice to be filed*

Attorneys for Plaintiff and the Proposed Class