NAILAH K. BYRD
CUYAHOGA COUNTY CLERK OF COURTS
1200 Ontario Street
Cleveland, Ohio 44113

Court of Common Pleas

AMENDED COMPLAINT $75
September 19, 2023 20:26

By: TERENCE R. COATES 0085579

Confirmation Nbr. 2968220

ANNMARIE GERO

vs.

MEDINFORM, INC.

CV 23 981382

Judge: RICHARD A. BELL

Pages Filed: 44

IN THE COURT OF COMMON PLEAS
CUYAHOGA COUNTY, OHIO

ANNMARIE GERO, **2082 Lark St., Apt. 2** **Lakewood, OH 44107,** **and** **TANAYA WILLIAMS** **1338 Washington Blvd.** **Mayfield Heights, OH 44124,** ***individually and on behalf of all others similarly situated,*** **Plaintiffs,** **v.** **MEDINFORM, INC.,** **6060 Rockside Woods Blvd. N., Suite 230** **Independence, OH 44131,** **Defendant.**	Case No.CV 23 981382 Judge Richard A. Bell **AMENDED CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

AMENDED CLASS ACTION COMPLAINT

Plaintiffs Annmarie Gero and Tanaya Williams (collectively "Plaintiffs"), individually and on behalf of all others similarly situated, bring this action against Defendant MedInform, Inc. (hereinafter known as "MedInform" or "Defendant"), an Ohio corporation, to obtain damages, restitution, and injunctive relief for the Class, as defined below, from Defendant. Plaintiffs make the following allegations upon information and belief, except as to their own actions, the investigation of their counsel, and the facts that are a matter of public record.

NATURE OF THE ACTION

1. This class action arises out of the recent targeted cyberattack and data breach ("Data Breach") on MedInform's network that resulted in unauthorized access to sensitive information

belonging to MedInform's clients' patients. As a result of the Data Breach, Plaintiffs and Class Members 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, Plaintiffs' and Class Members' sensitive personal information—which was entrusted to MedInform, and its officials and agents—was compromised and unlawfully accessed due to the Data Breach.

3. Information compromised in the Data Breach includes sensitive personal information such as names, addresses, Social Security numbers, medical billing information, and financial account information that Defendant MedInform collected and maintained (collectively the "PII"). Upon information and belief, the medical billing information compromised contains other sensitive information, such as treatment and diagnosis information, treatment and appointment dates, and treating physicians and facilities, as well as other such personal health information ("PHI" and together with PII, "Private Information").

4. Plaintiffs bring this class action lawsuit on behalf of those similarly situated to address Defendant's inadequate safeguarding of Class Members' Private Information that they collected and maintained, and for failing to provide timely and adequate notice to Plaintiffs and other 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. In particular, the Private Information was maintained on Defendant's computer system and network in a condition vulnerable to cyberattacks. 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, 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.

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

7. 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' 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.

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

9. 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.

10. By their Complaint, Plaintiffs seek to remedy these harms on behalf of themselves and all similarly situated individuals whose Private Information was accessed during the Data Breach.

11. Plaintiffs seek remedies including, but not limited to, compensatory damages, treble damages, punitive 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.

12. Accordingly, Plaintiffs bring this action against Defendant seeking redress for its unlawful conduct, and asserting claims for: (i) negligence, (ii) intrusion into seclusion/breach of privacy, (iii) negligence *per se*, (iv) breach of implied contract, (v) breach of fiduciary duty, and (vi) unjust enrichment.

JURISDICTION AND VENUE

13. This Court has subject matter jurisdiction over this action pursuant to R.C. § 2305.01, as the amount in controversy in this case exceeds $15,000. This Court has personal jurisdiction over Defendant MedInform because Defendant transacts business, contracts to supply services, and caused tortious injury by act or omission within the State of Ohio. In addition, Defendant is a domestic corporation in good standing, organized under the laws of Ohio, with a majority (if not all) of its business in the State of Ohio, thus rendering the exercise of personal jurisdiction by this Court necessary and proper.

14. Venue is proper in Cuyahoga County, Ohio under Ohio Rules of Civil Procedure Rule 3(C)(2) and 3(C)(3) because Defendant has its principal place of business and conducted the activities that gave rise to this claim in this county.

PARTIES

15. Plaintiff Annmarie Gero is, and at all times mentioned herein was, an individual citizen of the State of Ohio. Plaintiff was notified of the Data Breach and her Private Information being compromised upon receiving a data breach notice letter dated May 24, 2023. According to MedInform's notice on its website, dated May 24, 2023, the exposed data included Private

Information.[1]

16. Plaintiff Tanaya Williams is, and at all times mentioned herein was, an individual citizen of the State of Ohio. Plaintiff was notified of the Data Breach and her Private Information being compromised upon receiving a data breach notice letter on December 21, 2023. According to MedInform's notice on its website, dated May 24, 2023, the exposed data included Private Information.

17. Defendant MedInform, Inc. is a domestic corporation organized under the laws of the State of Ohio with its principal place of business located at 6060 Rockside Woods Blvd. N., Suite 230, Independence, Ohio 44131.

DEFENDANT'S BUSINESS

18. MedInform is a specialized provider of "accident recovery and itemization solutions" serving healthcare providers and hospital systems throughout Ohio.[2]

19. MedInform has been operating in Ohio since 2000, and is based in Independence, Ohio in Cuyahoga County.[3]

20. Defendant MedInform claims to specialize in providing its customers services related to accident recovery and itemization solutions. According to its website, these services are provided to hospital systems to assist with "recouping missed payments" and identifying sources of recovery for healthcare providers who have provided medical treatment and are seeking to recoup payment.[4]

---

[1] Home, MedInform, Inc. (May 24, 2023), https://www.medinforminc.com. (The Notice does not have a unique URL and is instead posted as pop-up window on MedInform's homepage.)

[2] *About*, MedInform, https://www.medinforminc.com/what-is-medinform/ (last visited June 14, 2023).

[3] *Id.*

[4] *Accident Recovery*, MedInform, https://www.medinforminc.com/accident-recovery/ (last visited June 14, 2023).

21. On information and belief, in the ordinary course of rendering its services to healthcare providers and hospital systems, MedInform requires its clients to turn over the private information of their patients, including information such as:

- Names, addresses, phone numbers, and email addresses;
- Dates of birth;
- Demographic information;
- Social Security numbers;
- Financial information;
- Information relating to individual medical history;
- Information concerning an individual's doctor, nurse or other medical providers;
- Photo identification;
- Employment information, and;
- Other information that may be deemed necessary.

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

23. Because of the highly sensitive and personal nature of the information Defendant acquires and stores with respect to its customers' patients, MedInform, upon information and belief, is aware of the importance of keeping individuals' Private Information confidential. It is also aware that it owes individuals whose Private Information it holds legal duties to comply with laws protecting customers' Private Information.

24. As a condition of obtaining services rendered from Defendant, MedInform requires

that its customers entrust it with highly sensitive personal information.

25. 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.

26. As a healthcare business associate, Defendant further owes duties to the individuals whose information it collects under federal laws such as the Health Insurance Portability and Accountability Act of 1996, commonly and hereinafter referred to as "HIPAA".

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

28. Plaintiffs and 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.

THE CYBERATTACK AND DATA BREACH

29. On December 21, 2022, MedInform became aware of a data security event, which resulted in the Data Breach that exposed Plaintiffs' and Class Members' Private Information.[5]

30. Upon learning of the security incident on December 21, 2022, MedInform launched an investigation into the incident to determine its "nature and scope."[6]

31. The investigation revealed that an unauthorized actor gained access to Defendant's system on or between December 5, 2022, and December 21, 2022, and that "certain information

[5] Home, MedInform, Inc. (May 24, 2023), https://www.medinforminc.com. (The Notice does not have a unique URL and is instead posted as pop-up window on MedInform's homepage.)

[6] *Id.*

was viewed or downloaded."[7]

32. The investigation further revealed that information compromised in the Data Breach included names, addresses, Social Security numbers, medical billing information, and financial account information.

33. While MedInform stated in its "Notice of Data Breach" letter that it learned of the cybersecurity incident on December 21, 2022, MedInform did not begin notifying victims until May 24, 2023 – approximately six months after discovering the Data Breach.[8]

34. In the Data Breach Notice posted on its website as a pop-up for customers, MedInform openly admits that files containing sensitive personal information were accessed during the Data Breach.[9] This means that not only did the cybercriminals view and access the Private Information without authorization, but that they also acquired Plaintiffs' and Class Members' Private Information from MedInform's computer network.

35. Plaintiffs' Private Information was stolen in the Data Breach. Plaintiffs further believe their Private Information was subsequently sold on the dark web following the Data Breach, as that is the *modus operandi* of all cybercriminals.

36. 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.

37. Plaintiffs and Class Members provided their Private Information, directly or

---

[7] *Id.*

[8] *See MedInform Sample Data Breach Notice Letter*, Montana Department of Justice, https://dojmt.gov/wp-content/uploads/Consumer-notification-letter-310.pdf (last visited June 14, 2022)

[9] Home, MedInform, Inc. (May 24, 2023), https://www.medinforminc.com. (The Notice does not have a unique URL and is instead posted as pop-up window on MedInform's homepage.) (last visited June 14, 2022)

indirectly, 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.

38. Defendant'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.

39. 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), Defendant knew or should have known that their electronic records would be targeted by cybercriminals.

40. Indeed, cyberattacks have become so notorious that the 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. . . because they often have lesser IT defenses and a high incentive to regain access to their data quickly."[10]

41. In fact, according to the cybersecurity firm Mimecast, 90% of healthcare

[10] *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 May 23, 2021).

organizations experienced cyberattacks in the past year.[11]

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

Defendant Fails to Comply with FTC Guidelines

43. 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.

44. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established cyber-security guidelines for businesses. The guidelines note that businesses should protect the personal customer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct any security problems.[12] 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.[13]

45. 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

---

[11] *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.

[12] *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 May 23, 2021).

[13] *Id.*

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.

46. 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.

47. These FTC enforcement actions include actions against healthcare related entities like Defendant. *See, e.g., In the Matter of Labmd, Inc., A Corp*, 2016-2 Trade Cas. (CCH) ¶ 79708, 2016 WL 4128215, at *32 (MSNET July 28, 2016) ("[T]he Commission concludes that LabMD's data security practices were unreasonable and constitute an unfair act or practice in violation of Section 5 of the FTC Act.")

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

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

50. Defendant was always fully aware of its obligation to protect the Private Information obtained from its customers. Defendant was also aware of the significant repercussions that would result from its failure to do so.

Defendant Fails to Comply with Industry Standards

51. As shown above, experts studying cyber security routinely identify entities

operating in the healthcare space as being particularly vulnerable to cyberattacks because of the value of the Private Information which they collect and maintain.

52. Several best practices have been identified that a minimum should be implemented by healthcare related entities 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.

53. 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.

54. 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.

55. 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 the cyber incident and causing the data breach.

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

56. HIPAA requires covered entities to protect against reasonably anticipated threats

to the security of sensitive patient health information.

57. Although Defendant is not a healthcare provider it is still a covered entity as a "business associate" of healthcare providers working with protected information obtained from healthcare providers for specific and narrow purposes.

58. Covered entities must implement safeguards to ensure the confidentiality, integrity, and availability of personal health information ("PHI") and other Private Information. Safeguards must include physical, technical, and administrative components.

59. Title II of HIPAA contains what are known as the Administrative Simplification provisions. 42 U.S.C. §§ 1301, *et seq*. These provisions require, among other things, that the Department of Health and Human Services ("HHS") create rules to streamline the standards for handling PII like the data Defendant left unguarded. The HHS subsequently promulgated multiple regulations under authority of the Administrative Simplification provisions of HIPAA. These rules include 45 C.F.R. § 164.306(a)(1-4); 45 C.F.R. § 164.312(a)(1); 45 C.F.R. § 164.308(a)(1)(i); 45 C.F.R. § 164.308(a)(1)(ii)(D), and 45 C.F.R. § 164.530(b).

60. A Data Breach such as the one Defendant experienced, is 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

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

DEFENDANT'S BREACH

62. Defendant breached its obligations to Plaintiffs and Class Members and/or was otherwise negligent and reckless because it failed to properly maintain and safeguard its computer

systems and data. Defendant's unlawful conduct includes, but is not limited to, the following acts and/or omissions:

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

b. Failing to adequately protect customers' 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 Private Information and maintain adequate email security practices;

f. Failing to ensure the confidentiality and integrity of electronic Private Information 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 Private Information 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 Private information in violation of 45 C.F.R. § 164.306(a)(2);

k. Failing to protect against reasonably anticipated uses or disclosures of electronic Private Information 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 Private Information as necessary and appropriate for the members of its workforces to carry out their functions and to maintain security of Private Information, in violation of 45 C.F.R. § 164.530(b);

n. Failing to render the electronic Private Information it maintained unusable, unreadable, or indecipherable to unauthorized individuals, as it had not encrypted the electronic Private Information 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.

63. Defendant negligently and unlawfully failed to safeguard Plaintiffs' and Class Members' Private Information by allowing cyberthieves to access MedInform's computer network and systems which contained unsecured and unencrypted Private Information.

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

65. Cyberattacks and data breaches at healthcare related businesses like Defendant are especially problematic because they can negatively impact the overall daily lives of individuals affected by the attack.

66. Researchers have found that among medical service providers that experience a data security incident, the death rate among patients increased in the months and years after the attack.[14]

67. Researchers have further found that at medical service providers that experienced a data security incident, the incident was associated with deterioration in timeliness and patient outcomes, generally.[15]

68. 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."[16]

---

[14] *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.

[15] *See* Sung J. Choi et al., *Data Breach Remediation Efforts and Their Implications for Hospital Quality*, 54 Health Services Research 971, 971-980 (2019). Available at https://onlinelibrary.wiley.com/doi/full/10.1111/1475-6773.13203.

[16] *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.

69. 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.

70. 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.[17]

71. 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.

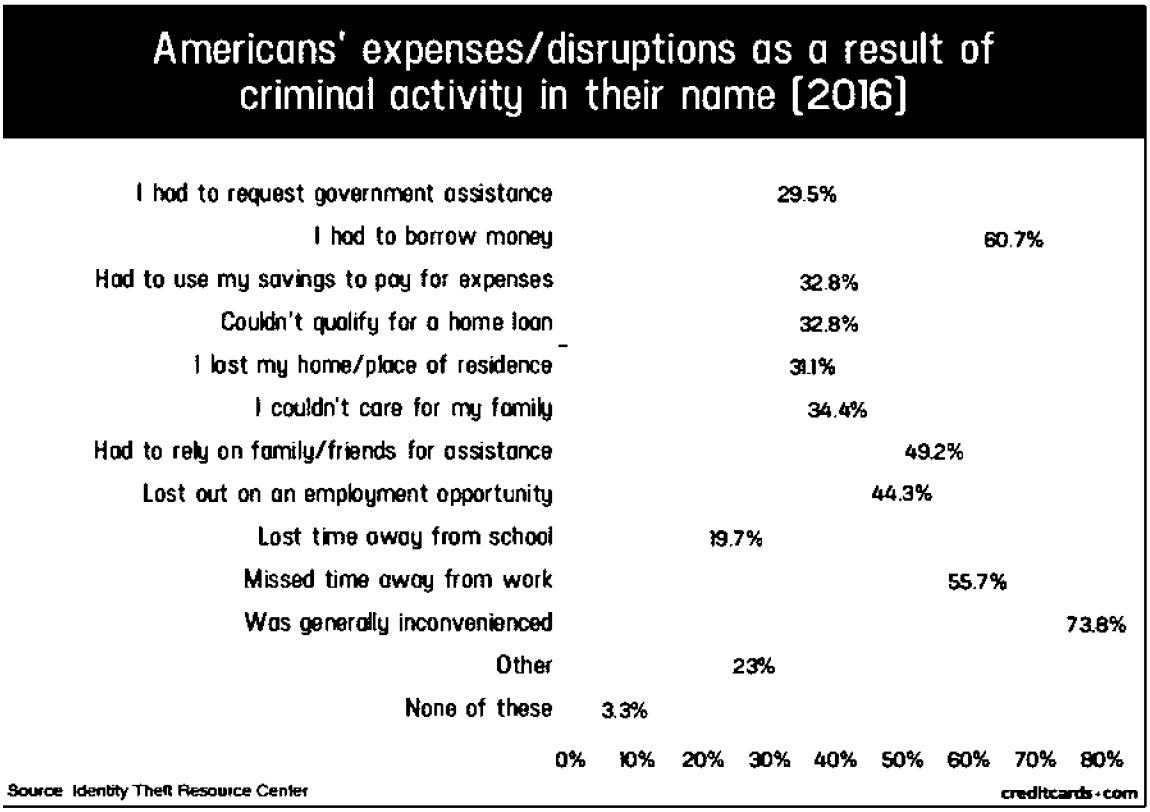
72. Identity thieves can also use Social Security numbers to obtain a driver's license or

---

[17] *See IdentityTheft.gov*, Federal Trade Commission, https://www.identitytheft.gov/Steps (last visited May 23, 2021).

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.

73. A study by Identity Theft Resource Center shows the multitude of harms caused by fraudulent use of personal and financial information:[18]



74. Moreover, theft of Private Information is also gravely serious. Private Information

[18] *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 May 27, 2021).

is an extremely valuable property right.[19]

75. 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.

76. Theft of PHI 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."[20]

77. Drug manufacturers, medical device manufacturers, pharmacies, hospitals and other healthcare service providers often purchase Private Information 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.

78. 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 between when Private Information and/or financial information is stolen and when it is used.

79. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches:

---

[19] *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).

[20] *See* Federal Trade Commission, *Medical Identity Theft*, http://www.consumer.ftc.gov/articles/0171-medical-identity-theft (last visited May 19, 2021).

> [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.

80. 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.

81. 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.

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

83. Sensitive Private Information can sell for as much as $363 per record according to the Infosec Institute.[21] 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.

84. 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.[22] 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

---

[21] *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/.

[22] *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 May 23, 2021).

unemployment benefits, or apply for a job using a false identity.[23] 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.

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

86. 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."[24]

87. 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."[25]

88. Medical information is especially valuable to identity thieves.

89. 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.[26] That

---

[23] *Id* at 4.

[24] 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.

[25] 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.

[26] *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/.

pales in comparison with the asking price for medical data, which was selling for $50 and up.[27]

90. 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.

91. For this reason, Defendant knew or should have known about these dangers and strengthened its data and email handling systems accordingly. Defendant was put on notice of the substantial and foreseeable risk of harm from a data breach, yet MedInform failed to properly prepare for that risk.

Plaintiffs' and Class Members' Damages

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

93. Defendant has merely offered Plaintiffs and Class Members complimentary fraud and identity monitoring services for up to twenty-four (24) months, but this does nothing to compensate them for damages incurred and time spent dealing with the Data Breach.

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

95. Plaintiffs' and Class Members' names, addresses, Social Security numbers, medical billing information, and financial account information were all compromised in the Data Breach and are now in the hands of the cybercriminals who accessed Defendant's computer system.

96. As a result of the Data Breach, Plaintiffs have experienced a substantial increase in suspicious scam phone calls which appear to be placed with the intent to obtain personal information to commit identity theft by way of a social engineering attack.

---

[27] 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.

97. Due to the Data Breach, Plaintiffs anticipate spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach.

98. Plaintiffs' Private Information was compromised as a direct and proximate result of the Data Breach.

99. 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.

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

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

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

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

104. Plaintiffs 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.

105. 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, directly or indirectly, to Defendant was intended to be used by Defendant to fund adequate security of MedInform's computer property and Plaintiffs' and Class Members' Private Information. Thus, Plaintiffs and Class Members did not get what they paid for and agreed to.

106. Plaintiffs and Class Members have spent and will continue to spend significant amounts of time monitoring their medical accounts and sensitive information for misuse.

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

a. Reviewing and monitoring sensitive accounts and finding fraudulent insurance claims, loans, and/or government benefits claims;

b. Purchasing credit monitoring and identity theft prevention;

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

d. Spending time on the phone with or at financial institutions, healthcare providers, and/or government agencies to dispute unauthorized and fraudulent activity in their name;

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

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

108. Moreover, Plaintiffs and Class Members have a continuing 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 Private Information is not accessible online and that access to such data is password protected.

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

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

CLASS ACTION ALLEGATIONS

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

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

> All persons MedInform identified as being among those individuals impacted by the Data Breach, including all who were sent a notice of the Data Breach (the "Class").
>
> All patients and/or customers MedInform identified as being among those individuals impacted by the Data Breach, including all who were sent a notice of the Data Breach (the "Customer Subclass").

113. Excluded from the Class and Subclass 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. Also excluded from the Class and Subclass are members of the judiciary to whom this case is assigned, their families and members of their staff.

114. Plaintiffs reserve the right to amend or modify the Class or Subclass definitions as this case progresses.

115. Numerosity. The Members of the Class are so numerous that joinder of all of them is impracticable. While the exact number of Class Members is unknown to Plaintiffs at this time, based on information and belief, the Class consists of approximately 14,453 individuals whose sensitive data was compromised in Data Breach.[28]

116. Commonality. There are questions of law and fact common to the Class, which predominate over any questions affecting only individual Class Members. These common questions of law and fact include, without limitation:

a. Whether Defendant unlawfully used, maintained, lost, or disclosed Plaintiffs' and Class Members' Private Information;

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

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

[28]https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf?adobe_mc=MCMID%3D02408406485458979789220680779370557994%7CMCORGID%3DA8833BC75245AF9E0A490D4D%2540AdobeOrg%7CTS%3D1685923200 (last visited; June 21, 2023).

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 Private Information;

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

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

h. Whether Defendant should have discovered the Data Breach sooner;

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

j. Whether Defendant's conduct was negligent;

k. Whether Defendant's acts, inactions, and practices complained of herein amount to acts of intrusion upon seclusion under the law;

l. Whether Defendant breached a fiduciary duty to Plaintiffs and Class Members;

m. Whether Defendant violated the consumer protection statute invoked below;

n. Whether Defendant breach implied contracts with Plaintiffs and Class Members;

o. Whether Defendant was unjustly enriched by unlawfully retaining a benefit conferred upon them by Plaintiffs and Class Members;

p. Whether Defendant failed to provide notice of the Data Breach in a timely manner, and;

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

117. Typicality. Plaintiffs' claims are typical of those of other Class Members because Plaintiffs' information, like that of every other Class Member, was compromised in the Data Breach.

118. Adequacy of Representation. Plaintiffs will fairly and adequately represent and protect the interests of the Members of the Class. Plaintiffs' Counsel are competent and experienced in litigating Class actions.

119. Predominance. Defendant has engaged in a common course of conduct toward Plaintiffs and Class Members, in that all the Plaintiffs' and Class Members' data was stored on the same computer system 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.

120. 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.

121. 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 and the Class)

122. Plaintiffs re-allege and incorporate by reference all other paragraphs in the Complaint as if fully set forth herein.

123. Defendant required its customers to submit the non-public Private Information of Plaintiffs and Class Members in the ordinary course of rendering its healthcare related business services.

124. By collecting and storing this data in its computer property, and sharing it and using it for commercial gain, Defendant owed 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 manner, and give prompt notice to those affected in the case of a data breach.

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

Private Information.

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

127. Defendant's duty to use reasonable security measures under HIPAA required Defendant to "reasonably protect" confidential data from "any intentional or unintentional use or disclosure" and to "have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information." 45 C.F.R. § 164.530(c)(1). Some or all of the medical information at issue in this case constitutes "protected health information" within the meaning of HIPAA.

128. 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.

129. Defendant's duty to use reasonable care in protecting confidential data arose not only because of the statutes and regulations described above, but also because Defendant is bound by industry standards to protect confidential Private Information.

130. 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. Failing to ensure that their email system had plans in place to maintain reasonable data security safeguards;

d. Failing to have in place mitigation policies and procedures;

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; and

g. 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.

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

132. 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.

133. Plaintiffs and Class Members are entitled to compensatory and consequential damages suffered because of the Data Breach.

134. Plaintiffs and Class Members are also entitled to injunctive relief requiring Defendant to, *e.g.,* (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
Intrusion Upon Seclusion / Invasion of Privacy
(On Behalf of Plaintiffs and the Class)

135. Plaintiffs repeat and re-allege every allegation contained in the Complaint as if fully set forth herein.

136. The State of Ohio also recognizes the tort of intrusion upon seclusion. This cause of action requires: (1) a wrongful intrusion, (2) into an individual's private affairs, (3) in such a way that would outrage or cause mental suffering, shame, or humiliation to a person of ordinary sensibilities. *See Miller v. Children's Hosp. Med. Ctr.*, 1st Dist. Hamilton No. C-050738, 2006-Ohio-3945, ¶ 14 (*citing Housh v. Peth*, 165 Ohio St. 35, 35, 133 N.E.2d 340, 341 (1956)).

137. Furthermore, according to the Court of Appeals of Ohio, Eighth District, Cuyahoga County, "[t]he tort of invasion of privacy protects persons from having their medical information released without their consent." *Rothstein v. Montefiore Home*, 116 Ohio App.3d 775, 780, 689 N.E. 2d 108 (8th Dist.1996) (*citing Levias v. United Airlines*, 27 Ohio App.3d 222, 500 N.E.2d 370 (8th Dist.1985).

138. Plaintiffs and Class Members had a reasonable expectation of privacy in the Private Information Defendant mishandled.

139. Defendant's conduct as alleged above intruded upon Plaintiffs' and Class Members' seclusion and privacy under common law.

140. By intentionally failing to keep Plaintiffs' and Class Members' Private Information safe, and by intentionally misusing and/or disclosing said information to unauthorized parties for unauthorized use, Defendant intentionally invaded Plaintiffs' and Class Members' privacy by:

a. Intentionally and substantially intruding into Plaintiffs' and Class Members' private affairs, without approval, in a manner that identifies Plaintiffs and Class Members and that would be highly offensive and objectionable to a person of ordinary sensibilities; and

b. Intentionally publicizing private facts about Plaintiffs and Class Members, which is highly offensive and objectionable to a person with ordinary sensibilities; and

c. Intentionally causing anguish or suffering to Plaintiffs and Class Members.

141. Defendant knew that an ordinary person in Plaintiffs' or a Class Member's position would consider Defendant's intentional actions highly offensive and objectionable.

142. Defendant invaded Plaintiffs' and Class Members' right to privacy and intruded into Plaintiffs' and Class Members' private life by intentionally misusing and/or disclosing their Private Information without their informed, voluntary, affirmative, and clear consent.

143. The Private Information disclosed by Defendant has no legitimate reason to be known by the public.

144. Defendant intentionally concealed from Plaintiffs and Class Members an incident that misused and/or disclosed their Private Information without their informed, voluntary, affirmative, and clear consent.

145. As a proximate result of such intentional misuse and disclosures, Plaintiffs' and Class Members' reasonable expectations of privacy in their Private Information was unduly frustrated and thwarted. Defendant's conduct, amounting to a substantial and serious invasion of Plaintiffs' and Class Members' protected privacy interests causing anguish and suffering such that a person with ordinary sensibilities would consider Defendant's intentional actions or inaction

highly offensive and objectionable.

146. In failing to protect Plaintiffs' and Class Members' Private Information, and in intentionally misusing and/or disclosing their Private Information, Defendant acted with intentional malice and oppression and in conscious disregard of Plaintiffs' and Class Members' rights to have such information kept confidential and private. Plaintiffs, therefore, seek an award of damages on behalf of themselves and the Class.

THIRD COUNT
Negligence *Per Se*
(On Behalf of Plaintiffs and the Class)

147. Plaintiffs repeat and re-allege every allegation contained in the Complaint as if fully set forth herein.

148. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendant's, of failing to use reasonable measures to protect Private Information. The FTC publications and orders described above also form part of the basis of Defendant's duty in this regard.

149. Defendant violated Section 5 of the FTC Act by failing to use reasonable measures to protect Private Information and not complying with applicable industry standards. Defendant's conduct was particularly unreasonable given the nature and amount of Private Information it obtained and stored, and the foreseeable consequences of the Data Breach for companies of Defendant's magnitude, including, specifically, the immense damages that would result to Plaintiffs and Members of the Class due to the valuable nature of the Private Information at issue in this case—including Social Security numbers.

150. Defendant's violations of Section 5 of the FTC Act constitute negligence *per se*.

151. Plaintiffs and members of the Class are within the class of persons that the FTC Act was intended to protect.

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

153. As a direct and proximate result of Defendants' negligence per se, Plaintiffs and members Class have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity how their PII is used; (iii) the compromise, publication, and/or theft of their PII; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from tax fraud and identity theft; (vi) costs associated with placing freezes on credit reports; (vii) the continued risk to their PII, which remains in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the PII of its current and former employees and customers in its 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 PII compromised as a result of the Data Breach for the remainder of the lives of Plaintiffs and members of the Class.

154. Additionally, as a direct and proximate result of Defendant's negligence *per se*, Plaintiffs and members of the Class have suffered and will suffer the continued risks of exposure

of 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 their continued possession.

FOURTH COUNT
Breach of Implied Contract
(On Behalf of Plaintiffs and the Customer Sub-class)

155. Plaintiffs repeat and re-allege every allegation contained in the Complaint as if fully set forth herein.

156. When Plaintiffs and Class Members provided their Private Information to MedInform, directly or indirectly, they entered into implied contracts with Defendant pursuant to which Defendant agreed to reasonably protect such information. Defendant received the benefit of their Private Information, along with the business of Defendant's clients, and Plaintiffs and Class Members received the benefit of Defendant's services along with the assurance that their Private Information would be duly protected.

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

158. 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.

159. 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.

160. Plaintiffs and Class Members would not have entrusted their Private Information to

Defendant in the absence of the implied contract between them and Defendant to keep their information reasonably secure. Plaintiffs and Class Members would not have entrusted their Private Information to Defendant in the absence of its implied promise to monitor its computer systems and networks to ensure that it adopted reasonable data security measures.

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

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

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

164. Plaintiffs and Class Members are entitled to compensatory and consequential damages suffered because of the Data Breach.

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

FIFTH COUNT
Breach of Fiduciary Duty
(On Behalf of Plaintiffs and the Customer Sub-class)

166. Plaintiffs repeat and re-allege every allegation contained in the Complaint as if fully set forth herein.

167. In light of the special relationship between Defendant and Plaintiffs and Class Members, whereby Defendant became guardians of Plaintiffs' and Class Members' Private Information, Defendant became a fiduciary by its undertaking and guardianship of the Private

Information, to act primarily for the benefit of its customers, including Plaintiffs and Class Members, as follows: (1) for the safeguarding of Plaintiffs' and Class Members' Private Information; (2) to timely notify Plaintiffs and Class Members of a data breach and disclosure; and (3) to maintain complete and accurate records of what customer information (and where) Defendant did and does store.

168. Defendant had a fiduciary duty to act for the benefit of Plaintiffs and Class Members upon matters within the scope of this relationship, and in particular, to keep secure the Private Information of its customers.

169. Defendant breached its fiduciary duties to Plaintiffs and Class Members by failing to diligently discover, investigate, and give notice of the Data Breach within a reasonable and practicable period.

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

171. Defendant breached its fiduciary duties owed to Plaintiffs and Class Members by failing to timely notify and/or warn Plaintiffs and Class Members of the Data Breach.

172. Defendant breached its fiduciary duties owed to Plaintiffs and Class Members by failing to ensure the confidentiality and integrity of electronic Private Information Defendant created, received, maintained, and transmitted, in violation of 45 C.F.R. § 164.306(a)(1).

173. Defendant breached its fiduciary duties owed to Plaintiffs and Class Members by failing to implement technical policies and procedures for electronic information systems that maintain electronic Private Information 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).

174. Defendant breached its fiduciary duties owed to Plaintiffs and Class Members by failing to implement policies and procedures to prevent, detect, contain, and correct security violations, in violation of 45 C.F.R. § 164.308(a)(1).

175. Defendant breached its fiduciary duties owed to Plaintiffs and Class Members by failing to identify and respond to suspected or known security incidents and to mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity in violation of 45 C.F.R. § 164.308(a)(6)(ii).

176. Defendant breached its fiduciary duties owed to Plaintiffs and Class Members by failing to protect against any reasonably-anticipated threats or hazards to the security or integrity of electronic Private Information in violation of 45 C.F.R. § 164.306(a)(2).

177. Defendant breached its fiduciary duties owed to Plaintiffs and Class Members by failing to protect against any reasonably anticipated uses or disclosures of electronic Private Information that are not permitted under the privacy rules regarding individually identifiable health information in violation of 45 C.F.R. § 164.306(a)(3).

178. Defendant breached its fiduciary duties owed to Plaintiffs and Class Members by failing to ensure compliance with the HIPAA security standard rules by its workforce in violation of 45 C.F.R. § 164.306(a)(94).

179. Defendant breached its fiduciary duties owed to Plaintiffs and Class Members by impermissibly and improperly using and disclosing Private Information that is and remains accessible to unauthorized persons in violation of 45 C.F.R. § 164.502, et seq.

180. Defendant breached its fiduciary duties owed to Plaintiffs and Class Members by failing to effectively train all Members of its workforce (including independent contractors) on the policies and procedures with respect to Private Information as necessary and appropriate for the

Members of its workforce to carry out their functions and to maintain security of Private Information in violation of 45 C.F.R. § 164.530(b) and 45 C.F.R. § 164.308(a)(5).

181. Defendant breached its fiduciary duties owed to Plaintiffs and Class Members by failing to design, implement, and enforce policies and procedures establishing physical and administrative safeguards to reasonably safeguard Private Information, in compliance with 45 C.F.R. § 164.530(c).

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

183. As a direct and proximate result of Defendant's breach 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 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 Data Breach for the remainder of the lives of Plaintiffs and Class Members; and (vii) the diminished value of Defendant's services they received.

184. As a direct and proximate result of Defendant's breaching its fiduciary duties,

Plaintiffs and Class Members have suffered and will continue to suffer other forms of injury and/or harm, and other economic and non-economic losses.

SIXTH COUNT
Unjust Enrichment
(On Behalf of Plaintiffs and the Customer Sub-Class)

185. Plaintiffs repeat and re-allege every allegation contained in the Complaint as if fully set forth herein.

186. This count is pleaded in the alternative to Count 4 (breach of implied contract).

187. Plaintiffs and Class Members conferred a monetary benefit on Defendant, directly or indirectly, by paying money for healthcare services, a portion of which went to Defendant for its business services and was to have been used for data security measures to secure Plaintiffs' and Class Members' Private Information, and by providing Defendant with their valuable Private Information.

188. Defendant enriched itself by saving the costs it reasonably should have expended on data security measures to secure Plaintiffs' and Class Members' Private Information. Instead of providing a reasonable level of security that would have prevented the Data Breach, Defendant instead calculated to avoid their data security obligations at the expense of Plaintiffs and Class Members by utilizing cheaper, ineffective security measures. Plaintiffs and Class Members, on the other hand, suffered as a direct and proximate result of Defendant's failure to provide the requisite security.

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

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

191. If Plaintiffs and Class Members knew that Defendant would not secure their Private Information, they would not have agreed to provide their Private Information to Defendant.

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

193. As a direct and proximate result of Defendant's conduct, Plaintiffs and Class Members have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity how their PII is used; (iii) the compromise, publication, and/or theft of their Private Information; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, and/or unauthorized use of their Private Information; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (vi) the continued risk to their 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 Private Information in their continued possession; and (vii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the Private Information compromised as a result of the Data Breach for the remainder of the lives of Plaintiffs and Class Members.

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

195. Defendant should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiffs and Class Members, proceeds that they unjustly received from

them. In the alternative, Defendant should be compelled to refund the amounts that Plaintiffs and Class Members overpaid for Defendant's services.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs pray for judgment as follows:

a) For an Order certifying this action as a Class action and appointing Plaintiffs as Class Representatives and their counsel as Class Counsel;

b) For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiffs' and Class Members' Private Information, and from refusing to issue prompt, complete and accurate disclosures to Plaintiffs and Class Members;

c) For equitable relief compelling Defendant to utilize appropriate methods and policies with respect to consumer data collection, storage, and safety, and to disclose with specificity the type of Private Information compromised during the Data Breach;

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

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

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

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

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

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

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

JURY TRIAL DEMANDED

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

Dated: September 19, 2023

Respectfully Submitted,

/s/ Terence R. Coates
Terence R. Coates (0085579)
Spencer Campbell (103001)
MARKOVITS, STOCK & DEMARCO, LLC
119 E. Court St., Ste. 530
Cincinnati, Ohio 4502
Phone: (513) 651-3700
Fax: (513) 665-0219
tcoates@msdlegal.com
scampbell@msdlegal.com

Philip J. Krzeski (0095713)
CHESTNUT CAMBRONNE PA
100 Washington Avenue South, Suite 1700
Minneapolis, MN 55401
Phone: (612) 339-7300
Fax: (612) 336-2940
pkrzeski@chestnutcambronne.com

Attorneys for Plaintiffs and the Proposed Class