IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF NEW YORK

PAUL COMMISSO and GLENDA JOHNSON, *individually and on behalf of all others similarly situated*, Plaintiffs, v. PROFESSIONAL BUSINESS SYSTEMS D/B/A PRACTICE*FIRST* MEDICAL MANAGEMENT SOLUTIONS, Defendant.	**Case No. _____** **CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

CLASS ACTION COMPLAINT

Plaintiffs, PAUL COMMISSO and GLENDA JOHNSON, individually and on behalf of all others similarly situated, brings this action against Defendant PROFESSIONAL BUSINESS SYSTEMS D/B/A PRACTICE*FIRST* MEDICAL MANAGEMENT SOLUTIONS ("Practice*First*" or "Defendant") 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 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 ransomware attack and data breach that was perpetrated against Defendant Practice*First*, a medical management company that processes

data for health care providers (the "Data Breach"). The Data Breach resulted in unauthorized access and exfiltration of highly sensitive and personal information (the "Private Information").

2. As a result of the Data Breach, Plaintiffs and approximately 1,210,688 Class Members[1] suffered present injury and damages in the form of identity theft, out-of-pocket expenses and the value of the time reasonably incurred to remedy or mitigate the effects of the unauthorized access, exfiltration, and subsequent criminal misuse of their sensitive and highly personal information.

3. The Private Information compromised in the Data Breach includes addresses, email addresses, dates of birth, driver's license numbers, Social Security numbers, diagnosis information, laboratory and treatment information, patient identification numbers, medication information, health insurance identification and claims information, tax identification numbers, and bank account and/or credit/debit card information.

4. The healthcare-specific data compromised is protected health information ("PHI") as defined by the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), and information such as Plaintiffs' Social Security number is deemed personally identifiable information ("PII").

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

[1] *See Cases Currently Under Investigation*, Office for Civil Rights, U.S. Dept. of Health and Human Services, https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf (last visited Aug. 9, 2021).

6. Upon information and belief, 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.

7. 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 the risk of a ransomware attack.

8. Plaintiffs' and Class Members' identities are now at considerable risk because of Defendant's negligent conduct since the PII and PHI that Practice*First* collected and maintained is now in the hands of data thieves.

9. Armed with the Private Information accessed in the Data Breach, data thieves can commit a variety of crimes, including but not limited to fraudulently applying for unemployment benefits, 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 (including unemployment or COVID relief benefits), filing fraudulent tax returns using Class Members' information, obtaining driver's licenses in Class Members' names but with another person's photograph and providing false information to police during an arrest.

10. 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. As a result of Defendant's actions and inactions, as set forth herein, Plaintiffs and Class Members must now and in the future closely

monitor their financial and medical accounts and information to guard against identity theft, among other issues.

11. Plaintiffs and Class Members have and may in the future incur actual monetary costs, including but not limited to the cost of purchasing credit monitoring services, credit freezes, credit reports or other protective measures to deter and detect identity theft.

12. Plaintiffs and Class Members have and may in the future expend time spent mitigating the effects of the Data Breach, including time spent dealing with actual or attempted fraud and identity theft.

13. By their Complaint, Plaintiffs seek to remedy these harms on behalf of himself and all similarly situated individuals whose PII and PHI was accessed during the Data Breach.

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

15. 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.

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

17. Accordingly, Plaintiffs brings this action against Defendant seeking redress for its unlawful conduct and asserts a claim for negligence.

PARTIES

18. Plaintiff Paul Commisso is, and at all times mentioned herein was, an individual citizen of the State of New York residing in the City of Akron.

19. Plaintiff Glenda Johnson is, and at all times mentioned herein was, an individual citizen of the State of New York residing in the City of Buffalo.

20. Defendant Practice*First* is a New York limited liability partnership with it its principal place of business at 50 Alcona Ave., Amherst, New York, 14228. Defendant Practice*First* is a medical service company specializing in coding, compliance, chart auditing, bookkeeping and tax preparation. It serves over 75 physician practices across the country and, consequently, maintains on its server network data for individuals who are patients of their clients from states other than the State of New York.

JURISDICTION AND VENUE

21. This Court has subject matter jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). There are at least 100 putative Class Members, the aggregated claims of the individual Class Members exceed the sum or value of $5,000,000 exclusive of interest and costs, and members of the proposed Class are citizens of states different from Defendant.

22. This Court has personal jurisdiction over Defendant Practice*First* as it is a domestic limited liability company in good standing, organized under the laws of the state of New York, with its principal place of business in Amherst, NY, rendering the exercise of personal jurisdiction by this Court proper and necessary.

23. Venue is proper because a substantial part of the events and omissions giving rise to these claims occurred in Erie County.

CLASS ACTION ALLEGATIONS

24. Plaintiffs brings this action on behalf of himself and on behalf of all other persons similarly situated (the "Class").

25. Plaintiffs proposes the following Class definition, subject to amendment as appropriate:

> All persons whose Private Information was compromised as a result of the Data Breach announced by Defendant Practice*First* on or about June 30, 2021 (the "Class").

26. Excluded from the Class are Defendant's officers and directors, and any entity in which Defendant has a controlling interest; and the affiliates, legal representatives, attorneys, successors, heirs, and assigns of Defendant. Excluded also from the Class are Members of the judiciary to whom this case is assigned, their families and Members of their staff.

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

28. 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 1,210,688 consumers whose data was compromised in the Data Breach.

29. 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;

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

i. Whether Defendant's conduct was negligent, and;

j. Whether Plaintiffs and Class Members are entitled to damages and/or injunctive relief.

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

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

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

33. 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.

34. 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.

35. Likewise, particular issues under Rule 23(c)(4) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

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

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

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

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

e. Whether Defendant's failed to take commercially reasonable steps to safeguard consumer Private Information; and

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

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

THE RANSOMWARE ATTACK AND DATA BREACH

37. A ransomware attack is a type of malicious software that blocks access to a computer system or data, usually by encrypting it, until the victim pays a fee to the attacker.[2]

[2] *See What is Ransomware?*, Proofpoint, https://www.proofpoint.com/us/threat-reference/ransomware (last accessed Aug. 9, 2021).

38. On December 30, 2020, Defendant learned that an unauthorized actor had attempted to deploy ransomware to encrypt its system and copied files.[3]

39. Defendant engaged a forensic investigation firm to determine the nature and scope of this incident.

40. Defendant determined that the ransomware was introduced by an unknown individual or individuals outside of its organization who gained access to part of its network where Defendant stored files that contained employee information and the confidential patient information of its clients.[4]

41. Defendant's investigation further determined that, as a result of this incident, certain personal or protected health information was compromised, including names, addresses, email addresses, dates of birth, driver's license numbers, Social Security numbers, diagnosis information, laboratory and treatment information, patient identification numbers, medication information, health insurance identification and claims information, tax identification numbers, and bank account and/or credit/debit card information.[5]

42. The investigation revealed that 1,210,688 individuals were impacted by the Data Breach.[6]

43. Despite learning of the Data Breach on December 30, 2020, notification letters were not sent to affected patients until more than six months later, on or around June 30, 2021, and Defendant did not notify the Department of Health and Human Services' Office for Civil Rights until July 1, 2021.[7]

---

[3] *Notice of Security Incident*, Practice*First*, https://www.practicefirstsecure.com/security-incident (last accessed Aug. 9, 2021).
[4] *Id*.
[5] *Id*.
[6] *Supra*, note 1.
[7] *Id*.

44. Defendant openly admits that the PII and PHI of Plaintiffs and Class Members that was accessed without authorization and held hostage by hackers was indeed "acquired" by the cyberthieves who perpetrated the Ransomware Attack.[8] Defendant's Notice of Security Incident states the cybercriminals "copied some files from our system."[9] This means that not only did the cybercriminals view and access the Private Information without authorization, but they also removed Plaintiffs' and Class Members' Private Information from Practice*First*'s network.

45. Though Defendant claims that the "actor who took the copy has advised that the Information is destroyed and was not shared,"[10] computer experts have definitively stated that "Proof of deletion is not a thing."[11]

46. There is simply no way Defendant could possibly know that the hackers did not simply copy the data in another location before offering whatever "proof" hackers claimed showed that the original copy was deleted. That Defendant has put its trust in the very people responsible for the Ransomware Attack in the first place is a disaster in waiting.

47. Due to Defendant's incompetent security measures, Plaintiffs and the Class Members now face an increased risk of fraud and identity theft and must deal with that threat forever.

48. Defendant has obligations created by HIPAA, industry standards and common law, to keep Class Members' Private Information confidential and to protect it from unauthorized access and disclosure.

---

[8] *Supra*, note 3.
[9] *Id.*
[10] *Id.*
[11] *See* Keith Mukai, *ArbiterSports Was Hacked. Don't Use Them Ever Again*, Medium (Aug. 29, 2020), https://medium.com/@kdmukai_64726/arbitersports-was-hacked-dont-use-them-ever-again-fddea92bcd21 (last accessed Aug. 9, 2021)

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

50. Indeed, ransomware attacks, such as the one experienced by Defendant have become so notorious that the Federal Bureau of Investigation ("FBI") and U.S. Secret Service have issued a warning to potential targets so they are aware of, and prepared for, a potential attack.

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

52. 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 the 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 the Private Information of its employees and the confidential patient information of its clients;

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

d. Failing to ensure that vendors with access to Practice*First*'s protected health data employed reasonable security procedures;

e. 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);

f. 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);

g. 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);

h. 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);

i. 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);

j. 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);

k. Failing to ensure compliance with HIPAA security standard rules by Defendant's workforce in violation of 45 C.F.R. § 164.306(a)(4);

l. Failing to train all members of Defendant's workforce effectively on the policies and procedures regarding PHI as necessary and appropriate for the members of its workforce to carry out their functions and to maintain security of PHI, in violation of 45 C.F.R. § 164.530(b); and/or

m. Failing to render the electronic PHI it maintained unusable, unreadable, or indecipherable to unauthorized individuals, as it had not encrypted the

electronic PHI as specified in the HIPAA Security Rule by "the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key" (45 CFR 164.304 definition of encryption).

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

o. Failing to adhere to industry standards for cybersecurity.

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

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

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

55. Ransomware attacks such as this one are especially problematic because of the disruption they cause to the overall daily lives of victims affected by the attack.

56. Ransomware attacks also constitute data breaches in the traditional sense. For example, in a ransomware attack on the Florida city of Pensacola, and while the City was still recovering from the ransomware attack, hackers released 2GB of data files from the total 32GB of data that they claimed was stolen prior to encrypting the City's network with the maze ransomware.

In the statement given to a news outlet, the hackers said, "***This is the fault of mass media who writes that we don't exfiltrate data***…."[12]

57. Also, in a ransomware advisory, the Department of Health and Human Services informed entities covered by HIPAA that "when electronic protected health information (ePHI) is encrypted as the result of a ransomware attack, a breach has occurred because the ePHI encrypted by the ransomware was acquired (i.e., unauthorized individuals have taken possession or control of the information)."[13]

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

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

59. Other security experts agree that when a ransomware attack occurs, a data breach does as well, because such an attack represents a loss of control of the data within a network.[14]

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

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

---

[12] *Pensacola Ransomware: Hackers Release 2GB Data as a Proof*, Cisomag (Dec. 27, 2019), https://www.cisomag.com/pensacola-ransomware-hackers-release-2gb-data-as-a-proof/.

[13] *See Fact Sheet: Ransomware and HIPAA*, Health and Human Services, https://www.hhs.gov/sites/default/files/RansomwareFactSheet.pdf (last accessed August 9, 2021).

[14] *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.

covered entity or business associate must initiate its security incident and response and reporting procedures. See 45 C.F.R.164.308(a)(6).[15]

Defendant Fails to Comply with FTC Guidelines

61. 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.

62. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established cyber-security guidelines for businesses. These 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.[16]

63. 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.[17]

64. 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

[15] *Supra*, note 13.
[16] *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 Aug. 9, 2021).
[17] *Id*.

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

65. 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.

66. These FTC enforcement actions include actions against healthcare 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.")

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

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

69. Upon information and belief, Defendant was at all times fully aware of its obligation to protect the patient PII and PHI of its medical practice 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

70. As noted 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.

71. Several best practices have been identified that at 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. Defendant failed to follow these industry best practices, including a failure to implement multi-factor authentication.

72. 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. Defendant failed to follow these cybersecurity best practices, including failure to train staff.

73. 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.

74. 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

75. HIPAA requires covered entities and the business associates of covered entities to protect against reasonably anticipated threats to the security of sensitive patient health information.

76. Defendant Practice*First* is a business associate of a "covered entity" under HIPAA. Business associates of covered entities must implement safeguards to ensure the confidentiality, integrity, and availability of PHI. Safeguards must include physical, technical and administrative components.

77. 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).

78. 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.

79. Defendant's Data Breach resulted from a combination of insufficiencies that demonstrate Practice*First* failed to comply with safeguards mandated by HIPAA regulations.

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

80. Cyberattacks and data breaches at business associates of healthcare providers, like Defendant, are especially problematic because they can negatively impact the overall daily lives of individuals affected by the attack.

81. 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."[18]

82. 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.

83. 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.

84. The FTC recommends that identity theft victims take several steps to protect their

[18] *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.

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.[19]

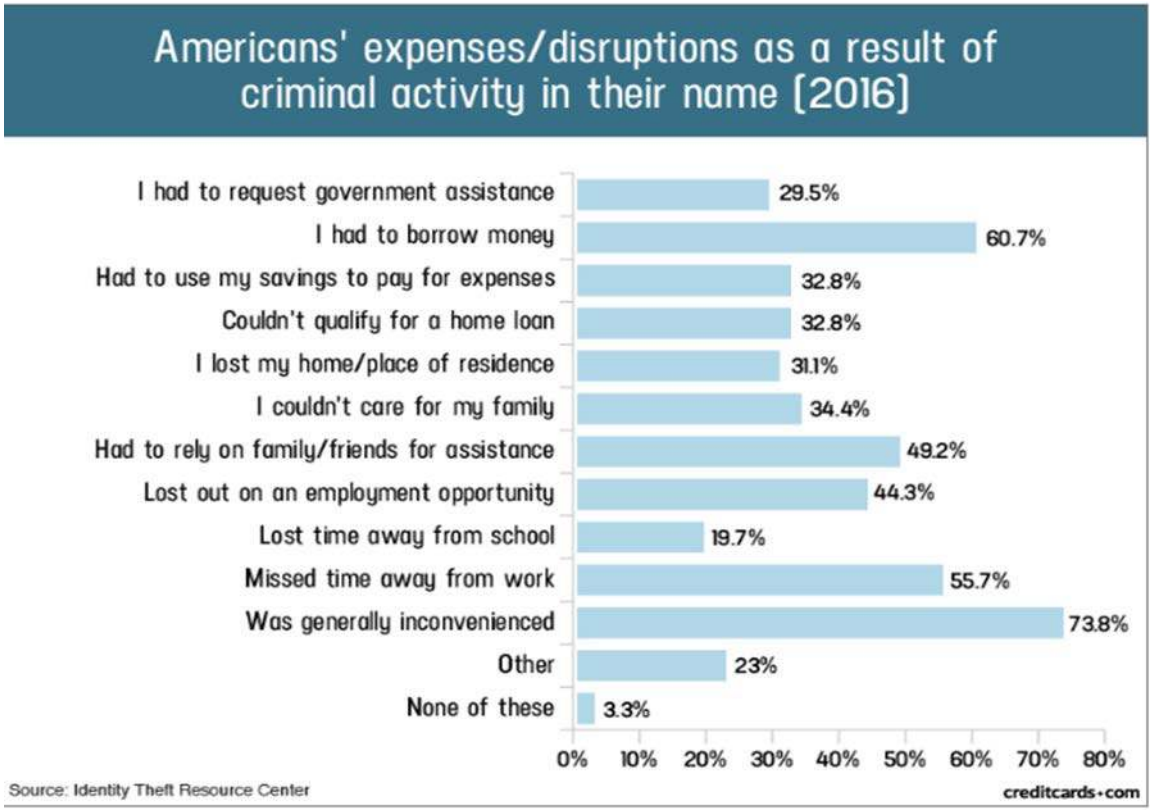
85. Identity thieves use stolen personal information such as Social Security numbers for a variety of crimes, including credit card fraud, phone or utilities fraud and bank/finance fraud.

86. 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.

87. 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.

88. A study by Identity Theft Resource Center shows the multitude of harms caused by fraudulent use of personal and financial information:[20]

[19] *See IdentityTheft.gov*, Federal Trade Commission, https://www.identitytheft.gov/Steps (last visited Aug. 9, 2021).
[20] *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.



89. Moreover, theft of Private Information is gravely serious; PII and PHI is an extremely valuable property right.[21]

90. 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.

91. 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

[21] *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).

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."[22]

92. 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.

93. Compounding issues for data breach victims is the fact that 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.

94. 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 29.

95. 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.

[22] *See Medical Identity Theft*, Federal Trade Commission, http://www.consumer.ftc.gov/articles/0171-medical-identity-theft (last visited Aug. 9, 2021).

96. 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.

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

98. Sensitive Private Information can sell for as much as $363 per record according to the Infosec Institute.[23]

99. 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.

100. 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.[24] Such fraud may go undetected until debt collection calls commence months, or even years, later.

101. 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.[25]

102. 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.

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

---

[23] *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/.

[24] *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 Aug. 9, 2021).

[25] *Id.* at 4.

104. 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."[26]

105. 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."[27]

106. Driver's license numbers are also incredibly valuable. "Hackers harvest license numbers because they're a very valuable piece of information. A driver's license can be a critical part of a fraudulent, synthetic identity – which go for about $1200 on the Dark Web. On its own, a forged license can sell for around $200."[28]

107. According to national credit bureau Experian:

> A driver's license is an identity thief's paradise. With that one card, someone knows your birthdate, address, and even your height, eye color, and signature. If someone gets your driver's license number, it is also concerning because it's connected to your vehicle registration and insurance policies, as well as records on file with the Department of Motor Vehicles, place of employment (that keep a copy of your driver's license on file), doctor's office, government agencies, and other entities. Having access to that one number can provide an identity thief with several pieces of information they want to know about you.

---

[26] 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.

[27] 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.

[28] Lee Mathews, *Hackers Stole Customers' License Numbers From Geico in Months-Long Beach*, Forbes (Apr, 20, 2021), https://www.forbes.com/sites/leemathews/2021/04/20/hackers-stole-customers-license-numbers-from-geico-in-months-long-breach/?sh=3e4755c38658.

> Next to your Social Security number, your driver's license number is one of the most important pieces of information to keep safe from thieves.[29]

108. According to cybersecurity specialty publication CPO Magazine, "[t]o those unfamiliar with the world of fraud, driver's license numbers might seem like a relatively harmless piece of information to lose if it happens in isolation."[30] However, this is not the case. As cybersecurity experts point out:

> "It's a gold mine for hackers. With a driver's license number, bad actors can manufacture fake IDs, slotting in the number for any form that requires ID verification, or use the information to craft curated social engineering phishing attacks."[31]

109. Victims of driver's license number theft also often suffer unemployment benefit fraud, as described in a recent New York Times article.[32]

110. Medical information is especially valuable to identity thieves.

111. 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.[33] That pales in comparison with the asking price for medical data, which was selling for $50 and up.[34]

112. 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.

---

[29] Sue Poremba, *What Should I Do If My Driver's License Number is Stolen?*, Experian (October 24, 2018) https://www.experian.com/blogs/ask-experian/what-should-i-do-if-my-drivers-license-number-is-stolen/.

[30] Scott Ikeda, *Geico Data Breach Leaks Driver's License Numbers, Advises Customers to Watch Out for Fraudulent Unemployment Claims*, CPO Magazine (Apr. 23, 2021), https://www.cpomagazine.com/cyber-security/geico-data-breach-leaks-drivers-license-numbers-advises-customers-to-watch-out-for-fraudulent-unemployment-claims/.

[31] *Id.*

[32] *How Identity Thieves Took My Wife for a Ride,* NY Times, April 27, 2021, https://www.nytimes.com/2021/04/27/your-money/identity-theft-auto-insurance.html (last accessed Aug. 9, 2021)

[33] *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/.

[34] 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.

113. 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 Practice*First* failed to properly prepare for that risk.

Plaintiffs' and Class Members' Injury and Damages

114. Plaintiffs and Class Members have been injured and damaged by the compromise of their PII and PHI in the Data Breach.

115. Plaintiffs' names, dates of birth, Social Security numbers, driver's license numbers, and health insurance and claims information, among other PII and PHI was compromised in the Data Breach and is now in the hands of the cybercriminals who illegally accessed Defendant's confidential files. Class Members PII and PHI, as described above, was similarly compromised and is now in the hands of the same cyberthieves.

Plaintiff Commisso

116. Plaintiff Commisso typically takes measures to protect his Private Information, and is very careful about sharing his PII and PHI. He has never knowingly transmitted unencrypted PII or PHI over the internet or any other unsecured source.

117. Plaintiff Commisso stores any documents containing his PII and PHI in a safe and secure location. Moreover, he diligently chooses unique usernames and passwords for his online accounts.

118. On or about June 30, 2021, Plaintiff Commisso belatedly received a Notice of Data Breach letter from Defendant.

119. According to Defendant, and as indicated in Plaintiff Commisso's Notice of Data Breach letter, his full name and Social Security number, among other confidential Private

Information, was compromised in the Data Breach. *See* Exhibit A.

120. Since being notified of the Data Breach on or about June 30, 2021, Plaintiff Commisso has spent time monitoring his confidential accounts for fraud and dealing with the impact of the Data Breach, valuable time Plaintiffs otherwise would have spent on other activities, including but not limited to work and/or recreation. This time included time spent on the telephone and sorting through unsolicited spam, verifying the legitimacy of the Data Breach, exploring credit monitoring and identity theft insurance options, and self-monitoring his sensitive accounts. This time has been lost forever and cannot be recaptured.

121. Due to the Data Breach, Plaintiff Commisso anticipates spending time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach.

Plaintiff Johnson

122. Plaintiff Johnson typically takes measures to protect his Private Information, and is very careful about sharing his PII and PHI. He has never knowingly transmitted unencrypted PII or PHI over the internet or any other unsecured source.

123. Plaintiff Johnson stores any documents containing his PII and PHI in a safe and secure location. Moreover, he diligently chooses unique usernames and passwords for his online accounts.

124. On or about June 30, 2021, Plaintiff Johnson belatedly received a Notice of Data Breach letter from Defendant.

125. According to Defendant, and as indicated in Plaintiffs Johnson's Notice of Data Breach letter, her full name and Social Security number, among other confidential Private Information, was compromised in the Data Breach. *See* Exhibit B.

126. Since being notified of the Data Breach on or about June 30, 2021, Plaintiff Johnson

has spent time monitoring his confidential accounts for fraud and dealing with the impact of the Data Breach, valuable time Plaintiffs otherwise would have spent on other activities, including but not limited to work and/or recreation. This time included time spent on the telephone and sorting through unsolicited spam, verifying the legitimacy of the Data Breach, exploring credit monitoring and identity theft insurance options, and self-monitoring his sensitive accounts. This time has been lost forever and cannot be recaptured.

127. Due to the Data Breach, Plaintiff Johnson anticipates spending time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach.

128. 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.

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

130. Plaintiffs and Class Members face substantial risk of out-of-pocket fraud losses such as unemployment benefits unlawfully applied for, 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.

131. 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.

132. Plaintiffs and Class Members may also incur additional 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.

133. 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.

134. Plaintiffs and Class Members have spent and will continue to spend significant amounts of time mitigating the effect of actual and attempted fraud and identity theft, including:

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.

135. Moreover, Plaintiffs and Class Members have an interest in ensuring that their Private Information, which is believed to remain in the possession of Defendant, is protected from further breaches by the implementation of security measures and safeguards, including but not

limited to, making sure that the storage of data or documents containing Private Information is not accessible online and that access to such data is password protected.

136. 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.

137. 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.

CAUSE OF ACTION
FIRST COUNT
NEGLIGENCE
(On Behalf of Plaintiffs and All Class Members)

138. Plaintiffs re-alleges and incorporates by reference Paragraphs 1 through 137 above as if fully set forth herein.

139. 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.[35] 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 ransomware attack.

[35] *Wallace v. Health Quest Sys., Inc.,* No. 20 Civ. 545 (VB), 2021 WL 1109727, at *9 (S.D.N.Y. Mar. 23, 2021) (finding that plaintiff plausibly pleaded that an operator of hospitals and healthcare providers owed a duty of care to safeguard customers' and patients' sensitive personal information).

140. 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.

141. Defendant's duty of care to use reasonable security measures arose as a result of the special relationship that existed between it, a business associate, and the patients of its clients, healthcare providers, 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 ransomware attack or data breach.

142. HIPAA imposes a duty and an actionable standard of care for an ordinary negligence claim. The HIPAA Privacy Rule prohibits covered entities from using or disclosing personal health information except as permitted by regulation. 45 C.F.R. § 164.502(a). The HIPAA privacy restrictions also govern the business associates of covered entities. 45 C.F.R. § 160.102. Practice*First* is subject to the actionable standards of care established by HIPAA as a business associate of covered entities.

143. 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.

144. 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.

145. 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 was bound by industry standards to protect confidential Private Information.

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

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

B. Failing to adequately monitor the security of its networks and systems;

C. Failure to periodically ensure that its email system had plans in place to maintain reasonable data security safeguards;

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

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

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

147. 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 both the financial services and medical industry.

148. 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.

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

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

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs prays for judgment as follows:

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

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

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

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

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

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

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

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

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

JURY TRIAL DEMANDED

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

Dated: August 16, 2021

Respectfully submitted,

/s/ Todd S. Garber
Todd S. Garber, Esq.
FINKELSTEIN, BLANKINSHIP, FREI-PEARSON & GARBER, LLP
One North Broadway, Suite 900
White Plains, NY 10601
Tel: (914) 298-3283
www.fbfglaw.com

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 60630
Tel.: (312) 283-3814
gklinger@masonllp.com

**pro hac vice to be filed*

Attorneys for Plaintiffs