Elaine A. Ryan (AZ Bar #012870)
Colleen M. Auer (AZ Bar#014637)
AUER RYAN, P.C.
20987 N. John Wayne Parkway, #B104-374
Maricopa, AZ 85139
520-705-7332
eryan@auer-ryan.com
cauer@auer-ryan.com
Counsel for Plaintiffs
(Additional Counsel listed below)

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF ARIZONA

Robert Hogsed, Justin Knox, Flor Medina, Brenda Allen, and Katherine Witkowski, on behalf of themselves and others similarly situated, Plaintiffs, v. PracticeMax, Inc., a Delaware corporation, Defendant.	No. 2:22-cv-01261-PHX-DLR **CONSOLIDATED CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED** Assigned to the Hon. Douglas L. Rayes

Plaintiffs Robert Hogsed, Justin Knox, Flor Medina, Brenda Allen, and Katherine Witkowski ("Plaintiffs"), individually and on behalf of all others similarly situated, bring this action against Defendant PracticeMax, Inc. ("Defendant" or "PracticeMax"). The following allegations are based on Plaintiffs' knowledge, investigations of counsel, facts of public record, and information and belief.

NATURE OF THE ACTION

1. Plaintiffs seek to hold PracticeMax—a medical practice management firm—responsible for the injuries it inflicted on Plaintiffs and approximately 350,000 similarly situated persons ("Class Members"). PracticeMax's data security was impermissibly inadequate causing the present data breach ("Data Breach"). Accordingly, PracticeMax's negligent security exposed the personal information of Plaintiffs and those similarly situated to cybercriminals.

2. The data that PracticeMax exposed to cybercriminals was highly sensitive. The exposed data includes personal identifying information ("PII") like Social Security Numbers, names, addresses, dates of birth, employer identification numbers, employee identification numbers, driver's license numbers, state identification numbers, passport numbers, passwords, PINs, and financial information.[1]

3. Also, the exposed data includes personal health information ("PHI") like medical treatments, diagnoses, health insurance information, patient account numbers, and prescription information.[2]

4. PracticeMax collected PII and PHI (collectively "Private Information") and then maintained that sensitive data in in a negligent and/or reckless manner. As evidenced by the Data Breach, PracticeMax inadequately maintained its network—rendering it easy prey for cybercriminals.

5. Upon information and belief, the risk of the Data Breach was known to PracticeMax. Thus, PracticeMax was on notice that its inadequate data security created a heightened risk of exposure, compromise, and theft.

---

[1] *PracticeMax - ME – Notice of Data Event*, MAINE ATT'Y GEN. https://apps.web.maine.gov/online/aeviewer/ME/40/d0bb4f19-c5f8-431f-9276-a9e34ebc266a/f16cb692-6473-4b18-b4eb-7d4b800f1b9a/document.html (last accessed Oct. 20, 2022).

[2] *Id.*

6. After the Data Breach, PracticeMax failed to provide timely notice to the Plaintiffs and Class Members thereby exacerbating their injuries. PracticeMax's dilatory notice deprived Plaintiffs and Class Members of the chance to take speedy measures to protect themselves and mitigate harm. Simply put, PracticeMax impermissibly left Plaintiffs and Class Members in the dark thereby causing their injuries to fester and the damage to spread.

7. Even when PracticeMax finally notified Plaintiffs and Class Members of their exposure, PracticeMax failed to adequately describe what information was compromised.

8. Today, the identities of Plaintiffs and Class Members are in jeopardy—all because of PracticeMax's negligence. Specifically, Plaintiffs and Class Members now suffer from a present and continuing risk of fraud and identity theft. And now, Plaintiffs and Class Members must constantly monitor their financial accounts.

9. Armed with the Private Information stolen in the Data Breach, criminals can commit a litany of crimes. Specifically, criminals can now open new financial accounts in Class Members' names, take out loans using Class Members' identities, use Class Members' names to obtain medical services, use Class Members' health information to craft phishing and other hacking attacks based on Class Members' individual health needs, use Class Members' identities to obtain government benefits, file fraudulent tax returns using Class Members' information, obtain driver's licenses in Class Members' names (but with another person's photograph), and give false information to police during an arrest.

10. Plaintiffs and Class Members will likely suffer additional financial costs for purchasing necessary credit monitoring services, credit freezes, credit reports, or other protective measures to deter and detect identity theft.

11. Plaintiffs and Class Members have suffered—and will continue to suffer—from the loss of the benefit of their bargain, unexpected out-of-pocket expenses, lost or

diminished value of their Private Information, emotional distress, and the value of their time reasonably incurred to mitigate the fallout of the PracticeMax's Data Breach.

12. Through this action, Plaintiffs seek to remedy these injuries on behalf of themselves and all similarly situated individuals whose Private Information were exposed and compromised in the Data Breach.

13. Plaintiffs seeks remedies including, but not limited to, compensatory damages, treble damages, punitive damages, reimbursement of out-of-pocket costs, and injunctive relief—including improvements to PracticeMax's data security systems, future annual audits, and adequate credit monitoring services funded by PracticeMax.

14. Plaintiffs bring this action against PracticeMax and assert claims for: (1) negligence; (2) breach of implied contract; (3) unjust enrichment; (4) breach of fiduciary duty; (5) violations of Arizona's Consumer Fraud Act; (6) violations of Illinois' Consumer Fraud and Deceptive Business Practices Act; (7) violations of Tennessee's Identity Theft Deterrence Act; and (8) violations of the Tennessee Consumer Protection Act.

PARTIES

15. Plaintiff Robert Hogsed is a natural person and citizen of Oklahoma. He has no intention of moving to a different state in the immediate future.

16. Plaintiff Justin Knox is a natural person and citizen of Tennessee. He has no intention of moving to a different state in the immediate future.

17. Plaintiff Flor Medina is a natural person and citizen of Arizona. She resides in Tolleson, Arizona. She has no intention of moving to a different state in the immediate future.

18. Plaintiff Brenda Allen is a natural person and citizen of Florida. She resides in Land O Lakes, Florida. She has no intention of moving to a different state in the immediate future.

19. Plaintiff Katherine Witkowski is a natural person and citizen of Illinois. She has no intention of moving to a different state in the immediate future.

20. Defendant PracticeMax, Inc. is a Delaware Corporation with its principal place of business at 1440 E. Missouri Ave, Suite C-200, Phoenix, Arizona 85364. PracticeMax has additional facilities throughout the country, including, but not limited to Louisiana, New York, and Illinois.

JURISDICTION AND VENUE

21. This Court has original jurisdiction under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2), because this is a class action involving more than 100 putative class members and the amount in controversy exceeds $5,000,000, exclusive of interest and costs. And minimal diversity is established because Plaintiffs (and many members of the Class) are citizens of states different than Defendant's.

22. This Court has general personal jurisdiction over PracticeMax because PracticeMax's principal place of business and headquarters are in Phoenix, Arizona. PracticeMax regularly conducts substantial business in Arizona.

23. Venue is proper in this District under 28 U.S.C. §§ 1391(a)(2), 1391(b)(2), and 1391(c)(2) because a substantial part of the events and omissions giving rise to the claims emanated from activities within this District, and PracticeMax conducts substantial business in this District.

FACTUAL ALLEGATIONS

PracticeMax Collected and Stored the Private Information of Plaintiffs and Class Members

24. Defendant PracticeMax is a medical practice management firm. It provides billing, consulting, and registration services to hospitals and healthcare providers.

25. On information and belief, PracticeMax maintains records of its customers' patients' information such as patients' full names, Social Security Numbers, financial

account information and/or credit-card information, dates of birth, prescription information, diagnosis information, treatment information, treatment providers, health insurance information, medical information, and Medicare/Medicaid ID numbers, in the ordinary course of business. These records are stored on PracticeMax's computer systems.

26. Because of the highly sensitive and personal nature of the information Defendant acquires and stores, PracticeMax knows or reasonably should have known that it stores protected Private Information and must comply with healthcare industry standards related to data security and all federal and state laws protecting customers' and patients' Private Information, and provide adequate notice to customers if their PII or PHI is disclosed without proper authorization.

27. When PracticeMax collects this sensitive information, it promises in, among other places, its applicable privacy policy to use reasonable measures to safeguard the Private Information from theft and misuse.

28. PracticeMax boasts that, "PracticeMax is committed to protecting your privacy."[3] It also declares that "[w]e will not disclose personally identifiable information we collect from you to third parties without your permission except to the extent necessary."[4] Finally, PracticeMax promises that "[we] will use commercially reasonable efforts to promptly respond and resolve any problem."[5]

29. PracticeMax acquired, collected, and stored, and represented that it maintained reasonable security over Plaintiffs' and Class Members' Private Information.

30. On information and belief, PracticeMax acquired, *inter alia*, the following types of information: names, addresses, phone numbers, email addresses, dates of birth, demographic information, Social Security Numbers, financial information, medical history

---

[3] *Privacy Policy*, PRACTICEMAX, https://practicemax.com/privacy-policy/ (last accessed Oct. 20, 2022).

[4] *Id.*

[5] *Id.*

information, medication information, health insurance, photo identification, and employment information.

31. And PracticeMax may receive information from other individuals and/or organizations that are part of a patient's "circle of care," such as referring physicians, customers' other doctors, customers' health plan(s), close friends, and/or family members.

32. By obtaining, collecting, and storing Plaintiffs' and Class Members' Private Information, PracticeMax assumed legal and equitable duties and knew, or should have known, that it was thereafter responsible for protecting Plaintiffs' and Class Members' Private Information from unauthorized disclosure.

33. Plaintiffs and Class Members have taken reasonable steps to maintain the confidentiality of their Private Information, including but not limited to, protecting their usernames and passwords, using only strong passwords for their accounts, and refraining from browsing potentially unsafe websites.

34. Upon information and belief, Plaintiffs and Class Members relied on PracticeMax to keep their Private Information confidential and securely maintained, to use this information for business and healthcare purposes only, and to make only authorized disclosures of this information.

35. PracticeMax could have prevented the Data Breach by properly securing and encrypting and/or more securely encrypting its servers generally, as well as Plaintiffs' and Class Members' Private Information.

36. PracticeMax's negligence in safeguarding Plaintiffs' and Class Members' Private Information was exacerbated by repeated warnings and alerts directed to the increased need to protect and secure sensitive data, as evidenced by the trending data breach attacks in recent years.

37. The healthcare industry, in particular, has experienced a large number of high-profile cyberattacks even in just the short period preceding the filing of this Complaint, and cyberattacks, generally, have become increasingly more common. More healthcare data

breaches were reported in 2020 than in any other year, showing a 25% increase.[6] Additionally, according to the HIPAA Journal, the largest healthcare data breaches have been reported beginning in April 2021.[7]

38. In the context of data breaches, healthcare is "by far the most affected industry sector."[8] Further, cybersecurity breaches in the healthcare industry are particularly devastating, given the frequency of such breaches and the fact that healthcare providers maintain highly sensitive and detailed PII.[9] And according to the cybersecurity firm Mimecast, 90% of healthcare organizations experienced cyberattacks in the past year.[10]

39. Despite the prevalence of public announcements of data breaches and data security compromises, PracticeMax failed to take appropriate steps to protect Plaintiffs' and Class Members' Private Information from being compromised.

40. PracticeMax failed to properly monitor and log the ingress and egress of network traffic for malware, such as, ransomware.[11]

41. PracticeMax failed to properly monitor and log file access and modifications.[12]

---

[6] *2020 Healthcare Data Breach Report,* HIPAA JOURNAL (Jan. 19, 2021) https://www.hipaajournal.com/2020-healthcare-data-breach-report-us/.

[7] *April 2021 Healthcare Data Breach Report,* HIPAA JOURNAL (May 18, 2021) https://www.hipaajournal.com/april-2021-healthcare-data-breach-report/.

[8] Tenable Security Response Team, *Healthcare Security*, TENABLE (Mar. 10, 2021), https://www.tenable.com/blog/healthcare-security-ransomware-plays-a-prominent-role-in-covid-19-era-breaches.

[9] *See id.*

[10] *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.

[11] *See Notice of Data Incident*, MONTANA DEPT. OF JUSTICE https://media.dojmt.gov/wp-content/uploads/Consumer-Notification-Letter-242.pdf (last accessed Oct. 21, 2022) (identifying "ransomware on certain systems" and stating that "we cannot rule out the possibility of" "unauthorized access, acquisition, or disclosure of sensitive information").

[12] *Id.*

42. PracticeMax failed to ensure file integrity.[13]

43. PracticeMax failed to properly train its employees as to cybersecurity awareness and best practices, specifically, how to avoid, detect, and report email phishing attacks.[14]

44. PracticeMax failed to provide fair, reasonable, or adequate computer systems and data security practices to safeguard the Private Information of Plaintiffs and Class Members.

45. PracticeMax failed to timely and accurately disclose that Plaintiffs' and Class Members' Private Information had been improperly acquired or accessed.

46. PracticeMax knowingly disregarded standard information security principles, despite obvious risks, by allowing unmonitored and unrestricted access to unsecured Private Information.

47. PracticeMax failed to provide adequate supervision and oversight of the Private Information with which it was and is entrusted, in spite of the known risk and foreseeable likelihood of breach and misuse, which permitted an unknown third party to gather Private Information of Plaintiffs and Class Members, misuse the PHI/PII and potentially disclose it to others without consent.

48. Upon information and belief, PracticeMax failed to adequately train its employees to not store Private Information longer than absolutely necessary.

49. Upon information and belief, PracticeMax failed to implement procedures so that Private Information was maintained no longer than absolutely necessary.

[13] *See id.* (stating that "some of the data stored in our network was encrypted as a result of the ransomware").

[14] *See id.* (stating that "[t]he investigation also identified unauthorized access to a limited number of company email accounts").

50. Upon information and belief, PracticeMax failed to consistently enforce security policies aimed at protecting Plaintiffs' and the Class Members' Private Information.

51. Upon information and belief, PracticeMax failed to implement sufficient processes to quickly detect data breaches, security incidents, or intrusions.

52. Upon information and belief, PracticeMax failed to encrypt Plaintiffs' and Class Members' Private Information and monitor user behavior and activity to identify possible threats.

PracticeMax's Data Breach

53. On May 1, 2021, PracticeMax discovered a cyberattack of its systems. PracticeMax discovered that cybercriminals had unrestricted access to its files and systems from April 17, 2021, to May 5, 2021 (the "Data Breach" or "Breach"). And PracticeMax admits that it "cannot rule out the possibility" of "unauthorized access, acquisition, or disclosure of sensitive information."[15]

54. Upon information and belief, Plaintiffs and Class Members' Private Information were stolen during the Data Breach. And upon information and belief, some of the data stored in PracticeMax's network was encrypted by the criminals.

55. On information and belief, cybercriminals were able to breach PracticeMax's systems because PracticeMax did not maintain reasonable security safeguards or protocols to protect patients' Private Information, leaving it an unguarded target for theft and misuse. PracticeMax admits as much in its Breach Notice sent to victims: "we reviewed our existing policies and procedures and implemented additional safeguards to further our already stringent security policies and procedures and to secure the information in our systems."[16]

---

[15] *Notice of Data Incident*, MONTANA DEPT. OF JUSTICE https://media.dojmt.gov/wp-content/uploads/Consumer-Notification-Letter-242.pdf (last accessed Oct. 21, 2022).

[16] *Data Breach Notifications*, MAINE ATT'Y GEN. https://apps.web.maine.gov/online

56. Simply put, Defendant should have implemented those "additional safeguards" years ago—thereby preventing the Data Breach and all of Plaintiffs and Class Members' injuries.

57. While PracticeMax claims to have become aware of the breach as early as May 1, 2021, PracticeMax did not begin notifying victims of the Data Breach until October 19, 2021.[17] PracticeMax did not inform other victims of the Data Breach until June 2022, over a full year after the Breach.

58. Upon information and belief, PracticeMax initially identified and notified only 500 individuals affected by the Data Breach.[18] Upon information and belief, in March 2022, PracticeMax identified and notified an additional 165,198 individuals affected by the Data Breach.[19] And upon information and belief, it was not until June 2022 that PracticeMax identified and notified another 154,929 individuals affected by the Data Breach.[20]

59. PracticeMax knew or reasonably should have known in May of 2021 the total number of affected individuals affected by the Data Breach.

60. Time is of the essence when highly sensitive Private Information is subject to unauthorized access and/or acquisition. The disclosed, accessed, and/or acquired Private

---

/aeviewer/ME/40/f3f3fcf1-7bee-45cc-a959-5fb886bf6ee1.shtml (last accessed Oct. 20, 2022).

[17] *Notice of Data Incident*, MONTANA DEPT. OF JUSTICE https://media.dojmt.gov/wp-content/uploads/Consumer-Notification-Letter-242.pdf (last accessed Oct. 21, 2022).

[18] *Cases Currently Under Investigation*, U.S. DEPT. OF HEALTH AND HUMAN SERVS: OFFICE FOR CIVIL RIGHTS https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf;jsessionid=B6CD42A6983C6CF29BF83E0C7DEB0BA3 (last accessed Oct. 21, 2022).

[19] *Data Breach Notifications*, MAINE ATT'Y GEN. https://apps.web.maine.gov/online/aeviewer/ME/40/f3f3fcf1-7bee-45cc-a959-5fb886bf6ee1.shtml (last accessed Oct. 20, 2022).

[20] *Data Breach Notifications*, MAINE ATT'Y GEN. https://apps.web.maine.gov/online/aeviewer/ME/40/f3f3fcf1-7bee-45cc-a959-5fb886bf6ee1.shtml (last accessed Oct. 20, 2022).

Information of Plaintiffs and Class Members is likely available on the Dark Web. Hackers can access and then offer for sale the unencrypted, unredacted Private Information to criminals. Plaintiffs and Class Members are now subject to the present and continuing risk of fraud, identity theft, and misuse resulting from the possible publication of their Private Information, especially their Social Security Numbers and sensitive medical information, onto the Dark Web. Plaintiffs and Class Members now face a lifetime risk of identity theft, which is heightened here by unauthorized access, theft, and/or disclosure of thousands of Social Security Numbers and/or specific, sensitive medical information.

61. Following the Breach and recognizing that each Class Member is now subject to the present and continuing risk of identity theft and fraud, PracticeMax's Breach Notice encouraged Plaintiffs and Class Members to "to remain vigilant by reviewing documents for suspicious activity, including health insurance statements, explanation of benefits of letters, medical records, account statements and credit reports." PracticeMax also informed Plaintiffs and Class Members in the Breach Notice that they may "contact the three major credit reporting bureaus [] to request a free copy of [their] credit report." Such measures are insufficient to protect Plaintiffs and Class Members from the lifetime risks each now face. As another element of damages, Plaintiffs and Class Members seek a sum of money sufficient to provide to Plaintiffs and Class Members identity theft protective services for their respective lifetimes.

62. PracticeMax put the burden squarely on Plaintiffs and Class Members to take measures to protect themselves.

63. Time is a compensable and valuable resource in the United States. According to the U.S. Bureau of Labor Statistics, 55.5% of U.S.-based workers are compensated on an hourly basis, while the other 44.5% are salaried.[21]

[21] *Characteristics of minimum wage workers, 2020*, U.S. BUREAU OF LABOR STATISTICS https://www.bls.gov/opub/reports/minimum-wage/2020/home.htm#:~:text=In%202020%2C%2073.3%20million%20workers,wage%20of%20%247.25%20per%20hour (last accessed Oct. 21, 2022); *Average Weekly Wage Data*, U.S. BUREAU OF LABOR

64. According to the U.S. Bureau of Labor Statistics' 2018 American Time Use Survey, American adults have only 36 to 40 hours of "leisure time" outside of work per week;[22] leisure time is defined as time not occupied with work or chores and is "the time equivalent of 'disposable income.'"[23] Usually, this time can be spent at the option and choice of the consumer, however, having been notified of the Data Breach, consumers now have to spend hours of their leisure time self-monitoring their accounts, communicating with financial institutions and government entities, and placing other prophylactic measures in place to attempt to protect themselves.

65. Plaintiffs and Class Members are now deprived of the choice as to how to spend their valuable free hours and seek renumeration for the loss of valuable time as another element of damages.

66. Upon information and belief, the unauthorized third-party cybercriminals gained access to Plaintiffs' and Class Members' Private Information and financial information with the intent of engaging in misuse of the Private Information and financial information, including marketing and selling Plaintiffs' and Class Members' Private Information.

67. PracticeMax had and continues to have obligations created by HIPAA, reasonable industry standards, common law, state statutory law, and its own assurances and representations to keep Plaintiffs' and Class Members' Private Information confidential and to protect such Private Information from unauthorized access.

STATISTICS, *Average Weekly Wage Data,* https://data.bls.gov/cew/apps/table_maker/v4/table_maker.htm%23type=1&year=2021&qtr=3&own=5&ind=10&supp=0 (last accessed Aug. 2, 2022) (finding that on average, private-sector workers make $1,253 per 40-hour work week.).

[22] Cory Stieg, *You're spending your free time wrong — here's what to do to be happier and more successful*, CNBC https://www.cnbc.com/2019/11/06/how-successful-people-spend-leisure-time-james-wallman.html (Nov. 6, 2019).

[23] *Id.*

68. PracticeMax's Breach Notice letter, as well as its website notice, both omit the size and scope of the breach. PracticeMax has demonstrated a pattern of providing inadequate notices and disclosures about the Data Breach.

69. Plaintiffs and the Class Members remain, even today, in the dark regarding what particular data was stolen, the particular ransomware used, and what steps are being taken, if any, to secure their Private Information and financial information going forward. Plaintiffs and Class Members are left to speculate as to the full impact of the Data Breach and how exactly PracticeMax intends to enhance its information security systems and monitoring capabilities so as to prevent further breaches.

70. Plaintiffs' and Class Members' Private Information and financial information may end up for sale on the dark web, or simply fall into the hands of companies that will use the detailed Private Information and financial information for targeted marketing without the approval of Plaintiffs and/or Class Members. Either way, unauthorized individuals can now easily access the Private Information and/or financial information of Plaintiffs and Class Members.

PracticeMax Failed to Comply with FTC Guidelines

71. According to the Federal Trade Commission ("FTC"), the need for data security should be factored into all business decision-making.[24] To that end, the FTC has issued numerous guidelines identifying best data security practices that businesses, such as PracticeMax, should employ to protect against the unlawful exposure of Personal Information.

72. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established guidelines for fundamental data security principles and practices for business.[25] The guidelines explain that businesses should:

[24] *Start with Security: A Guide for Business*, FED. TRADE COMM'N (June 2015), https://bit.ly/3uSoYWF (last accessed July 25, 2022).

[25] *Protecting Personal Information: A Guide for Business*, FED. TRADE COMM'N (Oct.

a. protect the personal customer information that they keep;

b. properly dispose of personal information that is no longer needed;

c. encrypt information stored on computer networks;

d. understand their network's vulnerabilities; and

e. implement policies to correct security problems.

73. The guidelines also recommend that businesses watch for large amounts of data being transmitted from the system and have a response plan ready in the event of a breach.

74. The FTC recommends that companies not maintain Private Information longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.[26]

75. 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.

76. These FTC enforcement actions include actions against healthcare providers and partners 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.").

2016), https://bit.ly/3u9mzre (last accessed July 25, 2022).

[26] *See Start with Security*, *supra* note 46.

77. PracticeMax's failure to employ reasonable and appropriate measures to protect against unauthorized access to patient Private Information constitutes an unfair act or practice prohibited by Section 5 of the FTCA, 15 U.S.C. § 45.

PracticeMax Failed to Follow Industry Standards

78. Despite its alleged commitments to securing sensitive patient data, PracticeMax does not follow industry standard practices in securing patients' Private Information.

79. As shown above, experts studying cyber security routinely identify healthcare providers as being particularly vulnerable to cyberattacks because of the value of the Private Information which they collect and maintain.

80. Several best practices have been identified that at a minimum should be implemented by healthcare providers like PracticeMax, 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.

81. 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.

82. PracticeMax 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.

83. Such frameworks are the existing and applicable industry standards in the healthcare industry. And PracticeMax failed to comply with these accepted standards—thus opening the door to criminals and the Data Breach.

PracticeMax Violated HIPAA

84. HIPAA circumscribes security provisions and data privacy responsibilities designed to keep patients' medical information safe. HIPAA compliance provisions, commonly known as the Administrative Simplification Rules, establish national standards for electronic transactions and code sets to maintain the privacy and security of protected health information.[27]

85. HIPAA provides specific privacy rules that require comprehensive administrative, physical, and technical safeguards to ensure the confidentiality, integrity, and security of Private Information is properly maintained.[28]

86. The Data Breach itself resulted from a combination of inadequacies showing PracticeMax failed to comply with safeguards mandated by HIPAA. PracticeMax's security failures include, but are not limited to:

a. Failing to ensure the confidentiality and integrity of electronic PHI that it creates, receives, maintains and transmits in violation of 45 C.F.R. § 164.306(a)(1);

[27] HIPAA lists 18 types of information that qualify as PHI according to guidance from the Department of Health and Human Services Office for Civil Rights, and includes, *inter alia*: names, addresses, any dates including dates of birth, Social Security Numbers, and medical record numbers.

[28] *See* 45 C.F.R. § 164.306 (security standards and general rules); 45 C.F.R. § 164.308 (administrative safeguards); 45 C.F.R. § 164.310 (physical safeguards); 45 C.F.R. § 164.312 (technical safeguards).

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

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

d. Failing to ensure compliance with HIPAA security standards by PracticeMax's workforce in violation of 45 C.F.R. § 164.306(a)(4);

e. 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);

f. 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);

g. Failing to identify and respond to suspected or known security incidents and failing 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);

h. Failing to effectively train all staff members on the policies and procedures with respect to PHI as necessary and appropriate for staff members to carry out their functions and to maintain security of PHI in violation of 45 C.F.R. § 164.530(b) and 45 C.F.R. § 164.308(a)(5); and

i. Failing to design, implement, and enforce policies and procedures establishing physical and administrative safeguards to reasonably safeguard PHI, in compliance with 45 C.F.R. § 164.530(c).

87. Simply put, the Data Breach resulted from a combination of insufficiencies that demonstrate PracticeMax failed to comply with safeguards mandated by HIPAA regulations.

The Experiences and Injuries of Plaintiffs

88. Plaintiffs and Class Members are the current and former patients of PracticeMax's customers. And as a prerequisite of receiving treatment, PracticeMax's customers require its patients—like Plaintiffs and Class Members—to disclose their Private Information.

89. PracticeMax began notifying victims about the Data Breach on or around October 19, 2021—over five months after discovering the breach. PracticeMax has provided additional notices of the breach since then, with the latest notice provided as recently as June 10, 2022. PracticeMax has failed to explain why it has taken over a year to notify all breach victims.

90. When PracticeMax finally announced the Data Breach, it deliberately underplayed the Breach's severity and obfuscated the nature of the Breach. PracticeMax's Breach Notice sent to patients fails to explain how many people were impacted, how the breach happened, or why it took over five months to send a barebones notice to impacted patients.

91. Normally, breached entities provide complimentary identity theft and credit monitoring services to their impacted parties. Not PracticeMax. PracticeMax refused to provide such basic protection services to its victims.[29] Instead, PracticeMax stated that they

[29] *Data Breach Notifications*, MAINE ATT'Y GEN. https://apps.web.maine.gov/online/aeviewer/ME/40/f3f3fcf1-7bee-45cc-a959-5fb886bf6ee1.shtml (last accessed Oct. 20, 2022).

are "providing impacted individuals with . . . a reminder to remain vigilant for incidents of fraud and identity theft . . . and encouragement to contact the Federal Trade Commission, their state Attorney General, and law enforcement to report attempted or actual identity theft and fraud."[30]

92. Because of the Data Breach, PracticeMax inflicted injuries upon Plaintiffs and Class Members. And yet, PracticeMax has done absolutely nothing to provide Plaintiffs and the Class Members with relief for the damages they suffered and will suffer.

93. All the Plaintiffs were injured when Defendant exposed their Private Information. Specifically, Defendant injured Plaintiffs by compromising, *inter alia*, medical treatments, diagnoses, health insurance information, patient account numbers, prescription information, Social Security Numbers, names, addresses, dates of birth, employer identification numbers, employee identification numbers, driver's license numbers, state identification numbers, passport numbers, passwords, PINs, and financial information.

94. Plaintiffs entrusted their Private Information to one of the entities that contracts services from PracticeMax. Upon information and belief, PracticeMax's agreements with those entities require it to protect and maintain the confidentiality of Private Information entrusted to it. Thus, Plaintiffs had the reasonable expectation and understanding that PracticeMax would take—*at minimum*—industry standard precautions to protect, maintain, and safeguard that information from unauthorized users or disclosure, and would timely notify them of any data security incidents. After all, Plaintiffs would not have entrusted their Private Information to any entity that used PracticeMax's services had

[30] *PracticeMax - ME – Notice of Data Event*, MAINE ATT'Y GEN. https://apps.web.maine.gov/online/aeviewer/ME/40/d0bb4f19-c5f8-431f-9276-a9e34ebc266a/f16cb692-6473-4b18-b4eb-7d4b800f1b9a/document.html (last accessed Oct. 20, 2022).

they known that PracticeMax would not take reasonable steps to safeguard their information.

95. Plaintiffs suffered actual injury from having their Private Information compromised because of the Data Breach including, but not limited to (a) damage to and diminution in the value of their Private Information—a form of property that PracticeMax obtained from Plaintiffs; (b) violation of their privacy rights; (c) the likely theft of their Private Information; (d) lost time spent investigating and addressing the effects of the Data Breach; (e) out of pocket expenses for credit monitoring; and (f) present and continuing injury arising from the present and continuing risk of identity theft and fraud.

96. As a result of the Data Breach, Plaintiffs also suffered emotional distress because of the release of their Private Information—which they believed would be protected from unauthorized access and disclosure. Now, Plaintiffs suffer from anxiety about unauthorized parties viewing, selling, and/or using their Private Information for nefarious purposes like identity theft and fraud.

97. And Plaintiffs also suffer anxiety about unauthorized parties viewing, using, and/or publishing their information related to their medical records and prescriptions.

98. Because of the Data Breach, Plaintiffs have spent—and will continue to spend—considerable time and money to try to mitigate and address harms caused by the Data Breach.

Plaintiff Hogsed's Experience

99. Plaintiff Hogsed received medical care and treatment resulting in billing and services from PracticeMax in the past. Upon information and belief, he was presented with standard medical forms to complete prior to his service that requested his Private Information, including HIPAA and privacy disclosure forms.

100. As part of his care and treatment, and as a requirement to receive Defendant's services, Plaintiff Hogsed entrusted his Private Information, and other confidential

information such as name, address, Social Security number, medical and treatment information, and health insurance information to PracticeMax with the reasonable expectation and understanding that PracticeMax would take at a minimum industry standard precautions to protect, maintain, and safeguard that information from unauthorized users or disclosure, and would timely notify him of any data security incidents related to him. Plaintiff would not have used PracticeMax's services had he known that PracticeMax would not take reasonable steps to safeguard his Private Information.

101. In June 2022, a full year after PracticeMax learned of the data breach, Plaintiff Hogsed received a letter from PracticeMax, dated June 13, 2022, notifying him that his Private Information had been improperly accessed and/or obtained by unauthorized third parties. The notice indicated that Plaintiff Hogsed's Private Information, including his name, address, date of birth, Social Security Number, financial information, medical treatment information, diagnosis information, and health insurance information was compromised as a result of the Data Breach.

102. As a result of the Data Breach, Plaintiff Hogsed made reasonable efforts to mitigate the impact of the Data Breach after receiving the data breach notification letter, including but not limited to researching the Data Breach reviewing credit card and financial account statements. He also intends to order a copy of his credit report and reach out to his insurance company to review those records as well to ensure that he has not been subject to any fraud. He is also in the process of changing passwords. He is also researching credit monitoring services to find an affordable option.

103. Plaintiff Hogsed has spent a few hours and will continue to spend valuable time he otherwise would have spent on other activities, including but not limited to work and/or recreation.

104. Plaintiff Hogsed suffered actual injury from having his Private Information compromised as a result of the Data Breach including, but not limited to (a) various

fraudulent charges on his debit card; (b) damage to and diminution in the value of his Private Information, a form of property that PracticeMax obtained from Plaintiff Hogsed; (c) violation of his privacy rights; (d) the likely theft of his Private Information; and (e) imminent and impending injury arising from the increased risk of identity theft and fraud.

105. As a result of the Data Breach, Plaintiff Hogsed has also suffered emotional distress as a result of the release of his Private Information, which he believed would be protected from unauthorized access and disclosure, including anxiety about unauthorized parties viewing, selling, and/or using his Private Information for purposes of identity theft and fraud. Plaintiff Hogsed is very concerned about identity theft and fraud, as well as the consequences of such identity theft and fraud resulting from the Data Breach. Plaintiff also has suffered anxiety about unauthorized parties viewing, using, and/or publishing his information related to his medical records and prescriptions.

106. As a result of the Data Breach, Plaintiff Hogsed anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. In addition, Plaintiff Hogsed will continue to be at present, imminent, and continued increased risk of identity theft and fraud for years to come.

Plaintiff Knox's Experience

107. Plaintiff Knox is a former patient of Fast Track Urgent Care, one of PracticeMax's customers.

108. Plaintiff Knox reasonably understood and expected that PracticeMax would safeguard his Private Information that it collected and stored on behalf of his medical provider and timely and adequately notify him in the event of a data breach. Plaintiff Knox would not have allowed PracticeMax, or anyone in Defendant's position, to maintain his Private Information if he believed that Defendant would fail to safeguard that information from unauthorized access.

109. In early August 2022, more than a year after the Data Breach, Plaintiff Knox received a letter from PracticeMax dated August 5, 2022, informing him that his Private Information—including his name, date of birth, medical billing and/or claims information, diagnosis, treatment information, physician's name, medical record name, health insurance information. and patient account number—was specifically identified as having been compromised in the Data Breach. The letter also identified other information on PracticeMax's systems at the time of the Breach that could have been exposed to cybercriminals. Thus, according to the letter, other information of Plaintiff Knox, including his Social Security Number, may have been accessed or stolen.

110. Despite acknowledging that the Data Breach had impacted his Private Information, PracticeMax did not even offer Plaintiff Knox any credit monitoring or identity theft protection.

111. Plaintiff Knox greatly values his privacy and takes reasonable steps to maintain the confidentiality of his Private Information. Plaintiff Knox is very concerned about identity theft and fraud, as well as the consequences of such identity theft and fraud resulting from the Data Breach. Plaintiff Knox is also very concerned about his private health information being accessed by unauthorized parties and potentially publicized.

112. Plaintiff Knox stores any and all documents containing his Private Information in a secure location and destroys any documents he receives in the mail that contain any Private Information or that may contain any information that could otherwise be used to compromise his identity private health information. Moreover, he diligently chooses unique usernames and passwords for his various online accounts.

113. To the best of his knowledge, Plaintiff Knox has never before been a victim of a data breach—until now.

114. As a result of the Data Breach notice, Plaintiff Knox spent approximately fifteen hours dealing with the consequences of the Data Breach, which includes time spent verifying the legitimacy of the Notice of Data Breach, placing freezes on his credit, and

self-monitoring his accounts and credit reports to ensure no fraudulent activity has occurred. Plaintiff Knox also spent time trying to call PracticeMax at the number provided on the breach notification letter in an attempt to get more information, but no one answered the phone. The time spent by Plaintiff Knox was valuable time that he otherwise would have spent on other activities, including but not limited to work and/or recreation.

115. The Data Breach has caused Plaintiff Knox to suffer fear, anxiety, and stress, which has been compounded by Defendant's year-long delay in noticing Plaintiff Knox of the fact that his Private Information were acquired by criminals as a result of the Data Breach. Plaintiff Knox's personal financial security has been jeopardized and there is uncertainty over what medical information was revealed in the Data Breach. This has been particularly disconcerting to Plaintiff Knox as he is in the process of trying to purchase a house.

116. Plaintiff Knox anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. In addition, Plaintiff Knox will continue to be at present, imminent, and continued increased risk of identity theft and fraud for years to come.

117. Plaintiff Knox suffers a present injury from the existing and continuing risk of fraud, identity theft, and misuse resulting from his Private Information being placed in the hands of criminals. Plaintiff Knox has a continuing interest in ensuring that his Private Information, which upon information and belief, remains in Defendant's possession, is protected and safeguarded from future breaches.

Plaintiff Medina's Experience

118. Plaintiff Medina is a former patient of one of PracticeMax's customers.

119. Plaintiff Medina reasonably understood and expected that PracticeMax would safeguard her Private Information that it collected and stored on behalf of her medical provider and timely and adequately notify her in the event of a data breach.

Plaintiff Medina would not have allowed PracticeMax, or anyone in Defendant's position, to maintain her Private Information if she believed that Defendant would fail to safeguard that information from unauthorized access.

120. In early June 2022, nearly a year after the Data Breach, Ms. Medina received a Breach Notice letter in the mail. That notice informed her that her Private Information were compromised. However, despite acknowledging that the Data Breach had impacted her Private Information, PracticeMax did not even offer Ms. Medina any credit monitoring or identity theft protection.

121. Plaintiff Medina greatly values her privacy and takes reasonable steps to maintain the confidentiality of her Private Information. Plaintiff Medina is very concerned about identity theft and fraud, as well as the consequences of such identity theft and fraud resulting from the Data Breach. Plaintiff Medina is also very concerned about her private health information being accessed by unauthorized parties and potentially publicized.

122. Plaintiff Medina stores any and all documents containing Private Information in a secure location and destroys any documents she receives in the mail that contain any PII or PHI or that may contain any information that could otherwise be used to compromise her identity private health information. Moreover, she diligently chooses unique usernames and passwords for her various online accounts.

123. To Plaintiff Medina's knowledge, her Private Information has not been compromised in a prior data breach.

124. As a result of the Data Breach notice, Ms. Medina spent more than 20 hours dealing with the consequences of the Data Breach, which includes time spent verifying the legitimacy of the Notice of Data Breach, researching the Data Breach, self-monitoring her accounts and credit reports to ensure no fraudulent activity has occurred, placing credit freezes on her accounts, and changing her passwords. This is valuable time Plaintiff spent that she otherwise would have spent on other activities, including but not limited to work and/or recreation.

125. And because of Data Breach, Ms. Medina received fraudulent calls from actors claiming to be from financial institutions, including Bank of America.

126. The Data Breach has caused Plaintiff Medina to suffer fear, anxiety, and stress, which has been compounded by Defendant's nine-month delay in noticing her of the fact that her Private Information were acquired by criminals as a result of the Data Breach. Ms. Medina's personal financial security has been jeopardized and there is uncertainty over what medical information was revealed in the Data Breach.

127. Plaintiff Medina anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. In addition, Plaintiff Medina will continue to be at present, imminent, and continued increased risk of identity theft and fraud for years to come.

128. Plaintiff Medina suffers a present injury from the existing and continuing risk of fraud, identity theft, and misuse resulting from her Private Information being placed in the hands of criminals. Plaintiff Medina has a continuing interest in ensuring that her Private Information, which upon information and belief, remains in Defendant's possession, is protected and safeguarded from future breaches.

Plaintiff Allen's Experience

129. Upon information and belief, Plaintiff Allen has been a patient of one of PracticeMax's customers.

130. Plaintiff Allen reasonably understood and expected that PracticeMax would safeguard her Private Information that it collected and stored on behalf of her medical provider and timely and adequately notify her in the event of a data breach. Plaintiff Allen would not have allowed PracticeMax, or anyone in Defendant's position, to maintain her Private Information if she believed that Defendant would fail to safeguard that information from unauthorized access.

131. On August 13, 2022, Ms. Allen received a Breach Notice letter in the mail, dated August 5, 2022.

132. Plaintiff Allen greatly values her privacy and takes reasonable steps to maintain the confidentiality of her Private Information. Plaintiff Allen is very concerned about identity theft and fraud, as well as the consequences of such identity theft and fraud resulting from the Data Breach. Plaintiff Allen is also very concerned about her private health information being accessed by unauthorized parties and potentially publicized.

133. Plaintiff Allen stores any and all documents containing Private Information in a secure location and destroys any documents she receives in the mail that contain any PII or PHI or that may contain any information that could otherwise be used to compromise her identity private health information. Moreover, she diligently chooses unique usernames and passwords for her various online accounts.

134. To Plaintiff Allen's knowledge, her Private Information has not been compromised in a prior data breach.

135. As a result of the Data Breach notice, Ms. Allen spent approximately five hours dealing with the consequences of the Data Breach, which includes time spent verifying the legitimacy of the Notice of Data Breach, exploring credit monitoring and identity theft insurance options, self-monitoring her accounts and credit reports to ensure no fraudulent activity has occurred, and seeking legal counsel regarding her options for remedying and/or mitigating the effects of the Data Breach. This time has been lost forever and cannot be recaptured.

136. As a result of and subsequent to the Data Breach, Ms. Allen has had an increase in spam emails and phone calls and received strange emails regarding medical issues and pre-recorded calls regarding Medicare coverage.

137. On August 24, 2022, Ms. Allen purchased credit monitoring and other services from Lifelock as a result of the Data Breach at a cost of $9.99 per month.

138. The costs of credit monitoring and other services purchased from Lifelock by Ms. Allen as a result of the Data Breach were both reasonable and necessary.

139. Ms. Allen suffered actual injury in the form of damages to and diminution in the value of her PHI/PII, a form of intangible property that she entrusted to Defendant, which was compromised in and as a result of the Data Breach.

140. Ms. Allen will have to spend considerable time and effort over the coming years monitoring her accounts to protect herself from identity theft. Ms. Allen's personal financial security has been jeopardized and there is uncertainty over what medical information was revealed in the Data Breach.

141. Ms. Allen suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach and has experienced anxiety and increased concerns for the loss of her privacy, as well as anxiety over the impact of cybercriminals accessing and using her PHI/PII and/or financial information.

142. Ms. Allen is now subject to the present and continuing risk of fraud, identity theft, and misuse resulting from her PHI/PII and financial information, in combination with her name, being placed in the hands of unauthorized third parties/criminals. This injury was worsened by Defendant's months-long delay in informing Plaintiffs and Class Members about the Data Breach.

143. Ms. Allen has a continuing interest in ensuring that her PHI/PII and financial information, which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future breaches.

144. Plaintiff Allen anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. In addition, Plaintiff Allen will continue to be at present, imminent, and continued increased risk of identity theft and fraud for years to come.

Plaintiff Witkowski's Experience

145. Plaintiff Witkowski is a former patient of one of PracticeMax's customers.

146. Plaintiff Witkowski reasonably understood and expected that PracticeMax would safeguard her PII and PHI that it collected and stored on behalf of her medical provider and timely and adequately notify her in the event of a data breach. Plaintiff Witkowski would not have allowed PracticeMax, or anyone in Defendant's position, to maintain her PII and PHI if she believed that Defendant would fail to safeguard that information from unauthorized access.

147. In early June 2022, nearly a year after the Data Breach, Ms. Witkowski received a Breach Notice letter in the mail. That notice informed her that her PII and PHI were compromised. However, despite acknowledging that the Data Breach had impacted her PII and PHI, PracticeMax did not even offer Ms. Witkowski any credit monitoring or identity theft protection. Indeed, Ms. Witkowski has had to pay for additional credit monitoring or other identity theft prevention since learning of the Data Breach.

148. Plaintiff Witkowski greatly values her privacy and takes reasonable steps to maintain the confidentiality of her PII and PHI. Plaintiff Witkowski is very concerned about identity theft and fraud, as well as the consequences of such identity theft and fraud resulting from the Data Breach. Plaintiff Witkowski is also very concerned about her private health information being accessed by unauthorized parties and potentially publicized.

149. Plaintiff Witkowski stores any and all documents containing PII and PHI in a secure location and destroys any documents she receives in the mail that contain any PII or PHI or that may contain any information that could otherwise be used to compromise her identity private health information. Moreover, she diligently chooses unique usernames and passwords for her various online accounts.

150. To Plaintiff Witkowski's knowledge, her PII and PHI has not been compromised in a prior data breach.

151. As a result of the Data Breach notice, Ms. Witkowski spent approximately 10-20 hours dealing with the consequences of the Data Breach, which includes time spent verifying the legitimacy of the Notice of Data Breach, self-monitoring her accounts and credit reports to ensure no fraudulent activity has occurred. This is valuable time Plaintiff spent that she otherwise would have spent on other activities, including but not limited to work and/or recreation.

152. And because of Data Breach, Ms. Witkowski received fraudulent texts, emails and calls from cybercriminals as well as an unsuccessful attempt by a cybercriminal to open a credit card in her name in 2021.

153. The Data Breach has caused Plaintiff Witkowski to suffer fear, anxiety, and stress, which has been compounded by Defendant's nine-month delay in noticing her of the fact that her PII and PHI were acquired by criminals as a result of the Data Breach. Ms. Witkowski's personal financial security has been jeopardized and there is uncertainty over what medical information was revealed in the Data Breach.

154. Plaintiff Witkowski anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. In addition, Plaintiff Witkowski will continue to be at present, imminent, and continued increased risk of identity theft and fraud for years to come.

155. Plaintiff Witkowski suffers a present injury from the existing and continuing risk of fraud, identity theft, and misuse resulting from her PII and PHI being placed in the hands of criminals. Plaintiff Witkowski has a continuing interest in ensuring that her PII and PHI, which upon information and belief, remains in Defendant's possession, is protected and safeguarded from future breaches.

Plaintiffs and the Proposed Class Face Significant Risk of Present and Continuing Identity Theft

156. Plaintiffs and Class Members suffered injury from the misuse of their Private Information that can be directly traced to PracticeMax.

157. The ramifications of PracticeMax's failure to keep Plaintiffs' and the Class's Private Information secure are severe. Identity theft occurs when someone uses another's personal and financial information such as that person's name, account number, Social Security Number, driver's license number, date of birth, and/or other information, without permission, to commit fraud or other crimes.

158. According to experts, one out of four data breach notification recipients become a victim of identity fraud.[31]

159. As a result of PracticeMax's failures to prevent—and to timely detect—the Data Breach, Plaintiffs and Class Members suffered and will continue to suffer damages, including monetary losses, lost time, anxiety, and emotional distress. They have suffered or are at a present risk of suffering:

a. The loss of the opportunity to control how their Private Information is used;

b. The diminution in value of their Private Information;

c. The compromise and continuing publication of their Private Information;

d. Out-of-pocket costs associated with the prevention, detection, recovery, and remediation from identity theft or fraud;

e. Lost opportunity costs and lost wages associated with the time and effort expended addressing and attempting to mitigate the actual and

[31] *More Than 12 Million Identity Fraud Victims in 2012 According to Latest Javelin Strategy & Research Report*, BUSINESSWIRE (Feb. 20, 2013) https://threatpost.com/study-shows-one-four-who-receive-data-breach-letter-become-fraud-victims-022013/77549/.

future consequences of the Data Breach, including, but not limited to, efforts spent researching how to prevent, detect, contest, and recover from identity theft and fraud;

f. Delay in receipt of tax refund monies;

g. Unauthorized use of stolen Private Information; and

h. The continued risk to their Private Information, which remains in the possession of PracticeMax and is subject to further breaches so long as PracticeMax fails to undertake the appropriate measures to protect the Private Information in its possession.

160. Stolen Private Information is one of the most valuable commodities on the criminal information black market. According to Experian, a credit-monitoring service, stolen Private Information can be worth up to $1,000.00 depending on the type of information obtained.[32]

161. The value of Plaintiffs' and the proposed Class's Private Information on the black market is considerable. Stolen Private Information trades on the black market for years, and criminals frequently post stolen private information openly and directly on various "dark web" internet websites, making the information publicly available, for a substantial fee of course.

162. It can take victims years to spot or identify Private Information theft, giving criminals plenty of time to milk that information for cash.

163. One such example of criminals using Private Information for profit is the development of "Fullz" packages.[33]

---

[32] Brian Stack, *Here's How Much Your Personal Information Is Selling for on the Dark Web*, EXPERIAN (Dec. 6, 2017) https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/.

[33] "Fullz" is fraudster speak for data that includes the information of the victim, including, but not limited to, the name, address, credit card information, Social Security Number, date of birth, and more. As a rule of thumb, the more information you have on a victim, the more money can be made off those credentials. Fullz are usually pricier than

164. Cyber-criminals can cross-reference two sources of Private Information to marry unregulated data available elsewhere to criminally stolen data with an astonishingly complete scope and degree of accuracy in order to assemble complete dossiers on individuals. These dossiers are known as "Fullz" packages.

165. The development of "Fullz" packages means that stolen Private Information from the Data Breach can easily be used to link and identify it to Plaintiff's and the proposed Class's phone numbers, email addresses, and other unregulated sources and identifiers. In other words, even if certain information such as emails, phone numbers, or credit card numbers may not be included in the Private Information stolen by the cyber-criminals in the Data Breach, criminals can easily create a Fullz package and sell it at a higher price to unscrupulous operators and criminals (such as illegal and scam telemarketers) over and over. That is exactly what is happening to Plaintiffs and members of the proposed Class, and it is reasonable for any trier of fact, including this Court or a jury, to find that Plaintiff's and other members of the proposed Class's stolen Private Information is being misused, and that such misuse is fairly traceable to the Data Breach.

166. According to the FBI's Internet Crime Complaint Center (IC3) 2019 Internet Crime Report, Internet-enabled crimes reached their highest number of complaints and dollar losses that year, resulting in more than $3.5 billion in losses to individuals and business victims.

---

standard credit card credentials, commanding up to $100 per record or more on the dark web. Fullz can be cashed out (turning credentials into money) in various ways, including performing bank transactions over the phone with the required authentication details in-hand. Even "dead Fullz", which are Fullz credentials associated with credit cards that are no longer valid, can still be used for numerous purposes, including tax refund scams, ordering credit cards on behalf of the victim, or opening a "mule account" (an account that will accept a fraudulent money transfer from a compromised account) without the victim's knowledge. *See, e.g.*, Brian Krebs, *Medical Records For Sale in Underground Stolen From Texas Life Insurance Firm*, KREBS ON SECURITY, (Sep. 18, 2014) https://krebsonsecurity.com/tag/fullz/.

167. Further, according to the same report, "rapid reporting can help law enforcement stop fraudulent transactions before a victim loses the money for good." PracticeMax did not rapidly report to Plaintiffs and the Class that their Private Information had been stolen.

168. Victims of identity theft also often suffer embarrassment, blackmail, or harassment in person or online, and/or experience financial losses resulting from fraudulently opened accounts or misuse of existing accounts.

169. In addition to out-of-pocket expenses that can exceed thousands of dollars and the emotional toll identity theft can take, some victims have to spend a considerable time repairing the damage caused by the theft of their Private Information. Victims of new account identity theft will likely have to spend time correcting fraudulent information in their credit reports and continuously monitor their reports for future inaccuracies, close existing bank/credit accounts, open new ones, and dispute charges with creditors.

170. Further complicating the issues faced by victims of identity theft, data thieves may wait years before attempting to use the stolen Private Information. To protect themselves, Plaintiffs and the Class will need to remain vigilant against unauthorized data use for years or even decades to come.

171. The Federal Trade Commission ("FTC") has also recognized that consumer data is a new and valuable form of currency. In an FTC roundtable presentation, former Commissioner Pamela Jones Harbour stated that "most consumers cannot begin to comprehend the types and amount of information collected by businesses, or why their information may be commercially valuable. Data is currency."[34]

172. The FTC has also issued numerous guidelines for businesses that highlight the importance of reasonable data security practices. The FTC has noted the need to factor

[34] *Commissioner Pamela Jones Harbour: Remarks Before FTC Exploring Privacy Roundtable*, FED. TRADE COMMISSION (Dec. 7, 2009), https://www.ftc.gov/sites/default/files/documents/public_statements/remarks-ftc-exploring-privacy-roundtable/091207privacyroundtable.pdf.

data security into all business decision-making.[35] According to the FTC, data security requires: (1) encrypting information stored on computer networks; (2) retaining payment card information only as long as necessary; (3) properly disposing of personal information that is no longer needed; (4) limiting administrative access to business systems; (5) using industry-tested and accepted methods for securing data; (6) monitoring activity on networks to uncover unapproved activity; (7) verifying that privacy and security features function properly; (8) testing for common vulnerabilities; and (9) updating and patching third-party software.[36]

173. According to the FTC, unauthorized Private Information disclosures are extremely damaging to consumers' finances, credit history and reputation, and can take time, money, and patience to resolve the fallout.[37] The FTC treats 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(a) of the FTC Act (the "FTCA").

174. To that end, the FTC has issued orders against businesses that failed to employ reasonable measures to secure sensitive payment card data. *See In the matter of Lookout Services, Inc.*, No. C-4326, ⁋ 7 (June 15, 2011) ("[Defendant] allowed users to bypass authentication procedures" and "failed to employ sufficient measures to detect and prevent unauthorized access to computer networks, such as employing an intrusion detection system and monitoring system logs."); *In the matter of DSW, Inc.*, No. C-4157, ⁋ 7 (Mar. 7, 2006) ("[Defendant] failed to employ sufficient measures to detect

[35] *Start With Security, A Guide for Business*, FED. TRADE COMMISSION, https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf (last visited Oct. 21, 2022).

[36] *Id.*

[37] *See Taking Charge, What to Do If Your Identity is Stolen*, FED. TRADE COMMISSION, at 3 (2012), https://www.ojp.gov/ncjrs/virtual-library/abstracts/taking-charge-what-do-if-your-identity -stolen.

unauthorized access."); *In the matter of The TJX Cos., Inc.*, No. C-4227 (Jul. 29, 2008) ("[R]espondent stored . . . personal information obtained to verify checks and process unreceipted returns in clear text on its in-store and corporate networks[,]" "did not require network administrators . . . to use different passwords to access different programs, computers, and networks[,]" and "failed to employ sufficient measures to detect and prevent unauthorized access to computer networks . . ."); *In the matter of Dave & Buster's Inc.*, No. C-4291 (May 20, 2010) ("[Defendant] failed to monitor and filter outbound traffic from its networks to identify and block export of sensitive personal information without authorization" and "failed to use readily available security measures to limit access between instore networks . . ."). These orders, which all preceded the Data Breach, further clarify the measures businesses must take to meet their data security obligations. PracticeMax thus knew or should have known that its data security protocols were inadequate and were likely to result in the unauthorized access to and/or theft of Private Information.

175. The healthcare industry is a prime target for data breaches.

176. Over the past several years, data breaches have become alarmingly commonplace. In 2016, the number of data breaches in the U.S. exceeded 1,000, a 40% increase from 2015.[38] The next year, that number increased by nearly 45%.[39] The following year the healthcare sector was the second easiest "mark" among all major sectors and categorically had the most widespread exposure per data breach.[40]

---

[38] *Data Breaches Increase 40 Percent in 2016, Finds New Report From Identity Theft Resource Center and CyberScout*, IDENTITY THEFT RESOURCE CENTER (Jan. 19, 2017), https://bit.ly/30Gew91 [hereinafter "*Data Breaches Increase 40 Percent in 2016*"].

[39] *Data Breaches Up Nearly 45 Percent According to Annual Review by Identity Thegt Resource Center® and CyberScout®*, IDENTITY THEFT RESOURCE CENTER (Jan. 22, 2018), https://bit.ly/3jdGcYR [hereinafter "*Data Breaches Up Nearly 45 Percent*"].

[40] *2018 End-of-Year Data Breach Report*, IDENTITY THEFT RESOURCE CENTER (Feb. 20, 2019), https://www.idtheftcenter.org/wp-content/uploads/2019/02/ITRC_2018-End-of-Year-Aftermath_FINAL_V2_combinedWEB.pdf.

177. Data breaches within the healthcare industry continued to increase rapidly. According to the 2019 Healthcare Information and Management Systems Society Cybersecurity Survey, 68% of participating vendors reported having a significant security incident within the last 12 months, with a majority of those being caused by "bad actors."[41]

178. The healthcare sector reported the second largest number of breaches among all measured sectors in 2018, with the highest rate of exposure per breach.[42] Indeed, when compromised, healthcare related data is among the most sensitive and personally consequential. A report focusing on healthcare breaches found that the "average total cost to resolve an identity theft-related incident . . . came to about $20,000," and that the victims were often forced to pay out-of-pocket costs for healthcare they did not receive in order to restore coverage.[43] Almost 50 percent of the victims lost their healthcare coverage as a result of the incident, while nearly 30 percent said their insurance premiums went up after the event. Forty percent of the customers were never able to resolve their identity theft at all. Data breaches and identity theft have a crippling effect on individuals and detrimentally impact the economy as a whole.[44]

179. The healthcare industry has "emerged as a primary target because [it sits] on a gold mine of sensitive personally identifiable information for thousands of patients at any given time. From Social Security and insurance policies to next of kin and credit cards, no other organization, including credit bureaus, ha[s] so much monetizable information stored in their data centers."[45]

---

[41] *2019 HIMSS Cybersecurity Survey*, HEALTHCARE INFORMATION AND MANAGEMENT SYSTEMS SOCIETY, INC. (Feb. 8, 2019), https://bit.ly/3LJqUr6.

[42] *2018 End-of-Year Data Breach Report*, IDENTITY THEFT RESOURCE CENTER (Feb. 20, 2019), https://www.idtheftcenter.org/wp-content/uploads/2019/02/ITRC_2018-End-of-Year-Aftermath_FINAL_V2_combinedWEB.pdf.

[43] Elinor Mills, *Study: Medical Identity Theft Is Costly for Victims*, CNET (Mar. 3, 2010), https://cnet.co/33uiV0v.

[44] *Id.*

[45] Eyal Benishti, *How to Safeguard Hospital Data from Email Spoofing Attacks*, INSIDE

180. Charged with handling highly sensitive Personal Information including healthcare information, financial information, and insurance information, PracticeMax knew or should have known the importance of safeguarding the Personal Information that was entrusted to it. PracticeMax also knew or should have known of the foreseeable consequences if its data security systems were breached. This includes the significant costs that would be imposed on PracticeMax's customers' patients as a result of a breach. PracticeMax nevertheless failed to take adequate cybersecurity measures to prevent the Data Breach from occurring.

181. PracticeMax disclosed the Private Information of Plaintiffs and members of the proposed Class for criminals to use in the conduct of criminal activity. Specifically, PracticeMax opened, disclosed, and exposed the Private Information of Plaintiffs and members of the proposed Class to people engaged in disruptive and unlawful business practices and tactics, including online account hacking, unauthorized use of financial accounts, and fraudulent attempts to open unauthorized financial accounts (i.e., identity fraud), all using the stolen Private Information.

182. PracticeMax's use of outdated and insecure computer systems and software that are easy to hack, and its failure to maintain adequate security measures and an up-to-date technology security strategy, demonstrates a willful and conscious disregard for privacy, and has exposed the Private Information of Plaintiffs and potentially thousands of members of the proposed Class to unscrupulous operators, con artists, and outright criminals. PracticeMax certainly knew, or should have known, that the healthcare industry is particularly vulnerable to cyberattacks and that, as a result, it must take steps to protect the trove of Private Information it holds.

183. Yet, on information and belief, PracticeMax failed to implement even the most basic levels of cybersecurity.

DIGITAL HEALTH (Apr. 4, 2019), https://bit.ly/3x6fz08.

184. PracticeMax's failure to properly notify Plaintiffs and members of the proposed Class of the Data Breach then exacerbated Plaintiffs' and members of the proposed Class's injury by depriving them of the earliest ability to take appropriate measures to protect their Private Information and take other necessary steps to mitigate the harm caused by the Data Breach. It then failed to even provide the most basic of remedies-credit monitoring- to the breach victims, almost ensuring that they will suffer identity theft and further harm.

CLASS ACTION ALLEGATIONS

185. Plaintiffs bring this action on behalf of themselves and on behalf of all other persons similarly situated ("the Classes") under Fed. R. Civ. P. 23(b)(2), 23(b)(3), and 23(c)(4).

186. Plaintiffs proposes the following Class definitions, subject to amendment as appropriate:

> **All persons residing in the United States whose Private Information was compromised in the Data Breach, including all persons that Defendant sent a notice of the Data Breach to (the "Class").**
>
> **All persons residing in the State of Arizona whose Private Information was compromised in the Data Breach, including all persons that Defendant sent a notice of the Data Breach to (the "Arizona Sub-Class").**
>
> **All persons residing in the State of Illinois whose Private Information was compromised in the Data Breach, including all persons that Defendant sent a notice of the Data Breach to (the "Illinois Sub-Class").**
>
> **All persons residing in the State of Tennessee whose Private Information was compromised in the Data Breach, including all persons that Defendant sent a notice of the Data Breach to (the "Tennessee Sub-Class").**

187. Together the Arizona Sub-Class, the Illinois Sub-Class, and the Tennessee Sub-Class are referred to herein as the "State Sub-Classes."The Classes defined above are readily ascertainable from information in PracticeMax's possession. Thus, such identification of Class Members will be reliable and administratively feasible.

188. Excluded from the Classes are: (1) any judge or magistrate presiding over this action and members of their families; (2) Defendant, Defendant's subsidiaries, parents, successors, predecessors, affiliated entities, and any entity in which Defendant or its parent has a controlling interest, and their current or former officers and directors; (3) persons who properly execute and file a timely request for exclusion from the Class; (4) persons whose claims in this matter have been finally adjudicated on the merits or otherwise released; (5) Plaintiff's counsel and Defendant's counsel; and (6) the legal representatives, successors, and assigns of any such excluded persons.

189. Plaintiffs reserve the right to amend or modify the Class definitions—including potential Subclasses—as this case progresses.

190. Plaintiffs satisfy the numerosity, commonality, typicality, and adequacy requirements under Fed. R. Civ. P. 23.

191. **Numerosity**. The Class Members are numerous such that joinder is impracticable. While the exact number of Class Members is unknown to Plaintiffs at this time, based on information and belief, the Classes consists of hundreds of thousands of individuals whose Private Information were compromised by PracticeMax's Data Breach.

192. **Commonality**. There are many questions of law and fact common to the Classes. And these common questions predominate over any individualized questions of individual Class Members. These common questions of law and fact include, without limitation:

a. If PracticeMax unlawfully maintained, lost, or disclosed Plaintiffs' and Class Members' Private Information;

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

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

e. If PracticeMax owed a duty to Class Members to safeguard their Private Information;

f. If PracticeMax breached its duty to Class Members to safeguard their Private Information;

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

h. If PracticeMax should have discovered the Data Breach earlier;

i. If PracticeMax took reasonable measures to determine the extent of the Data Breach after it was discovered;

j. If PracticeMax's delay in informing Plaintiffs and Class Members of the Data Breach was unreasonable;

k. If PracticeMax's method of informing Plaintiffs and Class Members of the Data Breach was unreasonable;

l. If PracticeMax's conduct was negligent;

m. If Plaintiffs and Class Members were injured as a proximate cause or result of the Data Breach;

n. If Plaintiffs and Class Members suffered legally cognizable damages as a result of PracticeMax's misconduct;

o. If PracticeMax breached implied contracts with Plaintiffs and Class Members;

p. If PracticeMax violated the consumer protection statutes invoked herein;

q. If PracticeMax was unjustly enriched by unlawfully retaining a benefit conferred upon it by Plaintiffs and Class Members;

r. If PracticeMax failed to provide notice of the Data Breach in a timely manner, and;

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

193. **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. Moreover, all Plaintiffs and Class Members were subjected to PracticeMax's uniformly illegal and impermissible conduct.

194. **Adequacy of Representation**. Plaintiffs will fairly and adequately represent and protect the interests of the Members of the Classes. Plaintiffs' Counsel are competent and experienced in litigating complex class actions. Plaintiffs have no interests that conflict with, or are antagonistic to, those of the Classes.

195. **Predominance**. PracticeMax 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 exposed in the same way. The common issues arising from PracticeMax'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.

196. **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 PracticeMax. In contrast, the conduct of this action as a Class action presents far fewer management difficulties, conserves judicial resources, the parties' resources, and protects the rights of each Class Member.

197. The litigation of the claims brought herein is manageable. PracticeMax's uniform conduct, the consistent provisions of the relevant laws, and the ascertainable identities of Class Members demonstrates that there would be no significant manageability problems with prosecuting this lawsuit as a class action.

198. Adequate notice can be given to Class Members directly using information maintained in PracticeMax's records.

199. 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 those set forth above.

200. PracticeMax 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.

FIRST CAUSE OF ACTION
Negligence
(On behalf of Plaintiffs and the Class, or, in the alternative, the State Sub-Classes)

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

202. PracticeMax required customers, including Plaintiffs and Class Members, to submit non-public Private Information in the ordinary course of rendering medical billing, consulting, and registration services to hospitals and healthcare providers.

203. By collecting and storing this data in its computer system and network for its own commercial gain, PracticeMax owed a duty of care to use reasonable means to secure and safeguard its computer system—and Class Members' Private Information held within it—to prevent disclosure of the information, and to safeguard the information from theft. PracticeMax's duty included a responsibility to implement processes so it could detect a breach of its security systems in a reasonably expeditious period of time and to give prompt notice to those affected in the case of a data breach.

204. The risk that unauthorized persons would attempt to gain access to the Private Information and misuse it was foreseeable. Given that PracticeMax holds vast amounts of Private Information, it was inevitable that unauthorized individuals would at some point try to access PracticeMax's databases of Private Information.

205. After all, Private Information is highly valuable, and PracticeMax knew, or should have known, the risk in obtaining, using, handling, emailing, and storing the Private Information of Plaintiffs and Class Members. Thus, PracticeMax knew, or should have known, the importance of exercising reasonable care in handling the Private Information entrusted to it.

206. PracticeMax 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.

207. PracticeMax's duty of care to use reasonable security measures arose because of the special relationship that existed between PracticeMax and patients, which is recognized by laws and regulations including but not limited to HIPAA, as well as common law. PracticeMax 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.

208. Under HIPAA, PracticeMax had a duty to use reasonable security measures 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."[46] Some or all of the medical information at issue in this case constitutes "protected health information" within the meaning of HIPAA.[47]

209. Moreover, under HIPAA, Defendant had a duty to render the electronic Private Information that it maintained as unusable, unreadable, or indecipherable to unauthorized individuals. Specifically, the HIPAA Security Rule requires "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."[48]

210. Plaintiffs and Class members are within the class of persons that the HIPAA was intended to protect. And the injuries that PracticeMax inflicted on Plaintiffs and Class Members are precisely the harms that HIPAA guards against. After all, the Federal Health and Human Services' Office for Civil Rights ("OCR") has pursued enforcement actions against businesses which—because of their failure to employ reasonable data security measures for PHI— caused the very same injuries that Defendant inflicted upon Plaintiffs and Class Members.

211. Under § 17932 of the Health Information Technology for Economic and Clinical Health Act ("HITECH"), PracticeMax has duty to promptly notify "without unreasonable delay and in no case later than 60 calendar days after the discovery of a

[46] 45 C.F.R. § 164.530(c)(1).

[47] *Id*.

[48] 45 C.F.R. § 164.304 (defining encryption).

breach" the respective covered entities and affected persons so that the entities and persons can take action to protect themselves.[49]

212. Moreover, § 17932(a) of HITECH states that, "[a] covered entity that accesses, maintains, retains, modifies, records, stores, destroys, or otherwise holds, uses, or discloses unsecured protected health information (as defined in subsection (h)(1)) shall, in the case of a breach of such information that is discovered by the covered entity, notify each individual whose unsecured protected health information has been, or is reasonably believed by the covered entity to have been, accessed, acquired, or disclosed as a result of such breach."

213. And § 17932(b) of HITECH states that, "[a] business associate of a covered entity that accesses, maintains, retains, modifies, records, stores, destroys, or otherwise holds, uses, or discloses unsecured protected health information shall, following the discovery of a breach of such information, notify the covered entity of such breach. Such notice shall include the identification of each individual whose unsecured protected health information has been or is reasonably believed by the business associate to have been, accessed, acquired, or disclosed during such breach."

214. Under the Federal Trade Commission Act, PracticeMax had a duty to employ reasonable security measures. Specifically, this statute 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.[50]

215. Moreover, Plaintiffs and Class Members' injuries are precisely the type of injuries that the FTCA guards against. After all, the FTC has pursued numerous enforcement actions against businesses that—because of their failure to employ reasonable

[49] 42 U.S.C.A. § 17932(d)(1).

[50] 15 U.S.C. § 45.

data security measures and avoid unfair and deceptive practices—caused the very same injuries that Defendant inflicted upon Plaintiffs and Class Members.

216. Under the Arizona Data Breach Notification Act, PracticeMax has a duty to promptly notify affected persons so they can take action to protect themselves if "the investigation [of a potential data breach] results in a determination that there has been a security system breach, the person that owns or licenses the computerized data, within forty-five days after the determination, shall . . . [n]otify the individuals affected."[51]

217. Moreover, Plaintiffs and Class Members' injuries are precisely the type of injuries that the Arizona Data Breach Notification Act guards against.

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

219. PracticeMax owed Plaintiffs and members of the Class a duty to notify them within a reasonable time frame of any breach to their Private Information. Defendant also owed a duty to timely and accurately disclose to Plaintiffs and members of the Class the scope, nature, and occurrence of the Data Breach. This duty is necessary for Plaintiffs and Class Members to take appropriate measures to protect their Private Information, to be vigilant in the face of an increased risk of harm, and to take other necessary steps in an effort to mitigate the fallout of PracticeMax's Data Breach.

220. PracticeMax owed these duties to Plaintiffs and Class Members because they are members of a well-defined, foreseeable, and probable class of individuals whom PracticeMax knew or should have known would suffer injury-in-fact from its inadequate security protocols. After all, PracticeMax actively sought and obtained the Private Information of Plaintiffs and Class Members.

[51] A.R.S §§ 18-551, 18-552.

221. PracticeMax breached its duties, and thus was negligent, by failing to use reasonable measures to protect Class Members' Private Information. And but for PracticeMax's negligence, Plaintiffs and Class Members would not have been injured. The specific negligent acts and omissions committed by PracticeMax include, but are not limited to:

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

b. Failing to comply with—and thus violating—HIPAA and its regulations;

c. Failing to comply with—and thus violating—HITECH and its regulations;

d. Failing to comply with—and thus violating—FTCA and its regulations;

e. Failing to comply with—and thus violating—the Arizona Data Breach Notification Act and its regulations;

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

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

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

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

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

k. 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.

222. It was foreseeable that PracticeMax'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. 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.

223. Simply put, PracticeMax's negligence actually and proximately caused Plaintiffs and Class Members' actual, tangible, injuries-in-fact and damages. These injuries include, but are not limited to, the theft of their Private Information by criminals, improper disclosure of their Private Information, lost value of their Private Information, and lost time and money incurred to mitigate and remediate the effects of the Data Breach that resulted from and were caused by PracticeMax's negligence. Moreover, injuries-in-fact and damages are ongoing, imminent, and immediate.

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

225. Plaintiffs and Class Members are also entitled to injunctive relief requiring PracticeMax to, *e.g.,* (1) strengthen its data security systems and monitoring procedures; (2) submit to future annual audits of those systems and monitoring procedures; and (3) to provide adequate credit monitoring to all Class Members.

SECOND CAUSE OF ACTION
Breach of Implied Contract
(On behalf of the Plaintiffs and the Class or, in the alternative, the State-Sub-Classes)

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

227. Plaintiffs and the Class Members entered into implied contracts with Defendant under which Defendant agreed to safeguard and protect their Private

Information and to timely and accurately notify Plaintiffs and Class Members that their information had been breached and compromised.

228. Plaintiffs and the Class were required to and delivered their Private Information to Defendant as part of the process of obtaining services provided by Defendant's customers. Plaintiffs and Class Members paid money, or money was paid on their behalf, to Defendant in exchange for services.

229. Defendant accepted possession of Plaintiffs' and Class Members' Private Information for the purpose of providing medical, billing, consulting and registration services to its customers that serve Plaintiffs and Class Members.

230. In its written policies, Defendant expressly and impliedly promised to Plaintiffs and Class Members that it would only disclose protected information and other Private Information under certain circumstances, none of which related to a Data Breach as occurred in this matter.

231. The implied promise of confidentiality includes consideration beyond those pre-existing general duties owed under HIPAA or other state of federal regulations. The additional consideration included implied promises to take adequate steps to comply with specific industry data security standards and FTC guidelines on data security.

232. The implied promises include but are not limited to: (1) taking steps to ensure that any agents who are granted access to Private Information also protect the confidentiality of that data; (2) taking steps to ensure that the information that is placed in the control of its agents is restricted and limited to achieve an authorized medical purpose; (3) restricting access to qualified and trained agents; (4) designing and implementing appropriate retention policies to protect the information against criminal data breaches; (5) applying or requiring proper encryption; (6) multifactor authentication for access; and (7) other steps to protect against foreseeable data breaches.

233. Based on the implicit understanding, Plaintiffs and Class Members accepted PracticeMax's offers and provided PracticeMax with their Private Information via their healthcare providers.

234. Plaintiffs and Class Members would not have permitted their Private Information to be collected and stored by PracticeMax had they known that PracticeMax would not safeguard their Private Information, as promised, or provide timely notice of a data breach.

235. Plaintiffs and Class Members fully performed their obligations under their implied contracts with PracticeMax.

236. PracticeMax breached the implied contracts by failing to safeguard Plaintiffs' and Class Members' Private Information and by failing to provide them with timely and accurate notice of the Data Breach.

237. The losses and damages Plaintiffs and Class Members sustained (as described above) were the direct and proximate result of PracticeMax's breach of its implied contracts with Plaintiffs and Class members.

THIRD CAUSE OF ACTION
Unjust Enrichment
(On behalf of Plaintiffs and the Class or, in the alternative, the State Sub-Classes)

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

239. This cause of action is plead in alternative to the breach of implied contract theory.

240. Plaintiffs and Class Members conferred a monetary benefit on PracticeMax, by paying money to healthcare providers who relied on PracticeMax to render certain services, a portion of which was intended to have been used by PracticeMax for data security measures to secure Plaintiffs and Class Members' Private Information. Plaintiffs

and Class Members further conferred a benefit on PracticeMax by entrusting their Private Information to it and from which PracticeMax derived profits.

241. PracticeMax 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, PracticeMax chose to avoid its 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 PracticeMax's failure to provide adequate security.

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

243. PracticeMax acquired the monetary benefit, PII, and PHI through inequitable means in that it failed to disclose the inadequate security practices previously alleged and failed to maintain adequate data security.

244. If Plaintiffs and Class Members knew that PracticeMax had not secured their Private Information, they would not have agreed to give their money—or disclose their data—to PracticeMax's customers.

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

246. As a direct and proximate result of PracticeMax's conduct, Plaintiffs and Class Members have suffered—and will continue to suffer—a host of injuries, including but not limited to: (1) actual identity theft; (2) the loss of the opportunity to determine how their PII is used; (3) the compromise, publication, and/or theft of their Private Information; (4) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, and/or unauthorized use of their Private Information; (5) 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; (6) the continued risk to their Private Information, which remain in PracticeMax's possession and are subject to further unauthorized disclosures so long as PracticeMax fails to undertake appropriate and adequate measures to protect the Private Information in its possession; and (7) future expenditures of time, effort, and money that will be spent trying to prevent, detect, contest, and repair the impact of PracticeMax's Data Breach.

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

248. PracticeMax should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiffs and Class Members, proceeds that it unjustly received from Plaintiffs and Class Members. Alternatively, PracticeMax should be compelled to refund the amounts that Plaintiffs and Class Members overpaid for PracticeMax's services.

FOURTH CAUSE OF ACTION
Breach of Fiduciary Duty
(On behalf of Plaintiffs and the Class or, in the alternative, the State Sub-Classes)

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

250. A relationship existed between Plaintiffs, the Class Members, and PracticeMax, which arose from PracticeMax's acceptance of Plaintiffs' and the Class Members' Private Information and PracticeMax's representations of its commitment to protect said Private Information.

251. The interests of public policy mandate that a fiduciary duty is imputed given PracticeMax's acceptance of Plaintiffs' and the Class Members' Private Information and PracticeMax's representations of its commitment to protect said Private Information.

252. PracticeMax breached the fiduciary duty that it owed to Plaintiffs and Class Members. Specifically, because PracticeMax failed to act with the utmost good faith, fairness, honesty, and the highest and finest loyalty—and ultimately, by failing to protect the Private Information of Plaintiffs and Class Members.

253. PracticeMax's breach of fiduciary duty was a legal cause of damage to Plaintiffs and Class Members.

254. But for PracticeMax's breach of fiduciary duty, the damage to Plaintiffs and Class Members would not have occurred.

255. PracticeMax's breach of fiduciary duty contributed substantially to producing the damage to Plaintiffs and Class Members.

256. As a direct and proximate result of PracticeMax's breach of fiduciary duty, Plaintiffs and Class Members are entitled to and demand actual, consequential, nominal damages, and injunctive relief.

FIFTH CAUSE OF ACTION
Violations of the Arizona Consumer Fraud Act,
A.R.S. §§ 44-1521, *et seq.*
(On behalf of Plaintiffs and the Class, or alternatively, on behalf of Plaintiff Medina and the Arizona Sub-Class)

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

258. PracticeMax is a "person" as defined by A.R.S. § 44-1521(6).

259. PracticeMax sold Plaintiffs and Class Members "merchandise" as defined by A.R.S. § 44-1521, in the form of services, including medical billing and records services.

260. Section 44-1522 of the Arizona Consumer Fraud Act provides:

> The act, use or employment by any person of any deception, deceptive or unfair act or practice, fraud, false pretense, false promise, misrepresentation, or concealment, suppression or omission of any material fact with intent that others rely on such concealment, suppression or omission, in connection with the sale or advertisement of any merchandise whether or not any person has in fact been misled, deceived or damaged thereby.

A.R.S. § 44-1522(A).

261. PracticeMax used deception, used a deceptive act or practice, and fraudulently omitted and concealed material facts in connection with the sale or advertisement of that merchandise in violation of A.R.S. § 44-1522(A).

262. PracticeMax omitted and concealed material facts, which it knew about and had the duty to disclose, namely, PracticeMax's inadequate privacy and security protections for Plaintiffs' and Class Members' Private Information. This omission was designed to mislead consumers.

263. PracticeMax omitted and concealed those material facts even though in equity and good conscience those facts should have been disclosed and did so with the intent that others would rely on the omission, suppression, and concealment.

264. Upon information and belief, PracticeMax intentionally omitted and concealed material facts—like PracticeMax's inadequate cyber and data privacy and security protections—with the intention that consumers rely on those omissions.

265. The concealed facts are material in that they are logically related to the transactions at issue and rationally significant to the parties in view of the nature and circumstances of those transactions.

266. Plaintiffs and Class Members were ignorant of the truth and relied on the concealed facts in providing Private Information to PracticeMax and incurred damages as a consequent and proximate result.

267. But for PracticeMax's omissions, the damage to Plaintiffs and Class Members would not have occurred.

268. Plaintiffs do not allege any claims based on any affirmative misrepresentations by PracticeMax. Rather, Plaintiffs allege that PracticeMax omitted, failed to disclose, and concealed material facts and information as alleged herein—despite its duty to disclose such facts and information.

269. PracticeMax knew or should have known that its computer system and data security practices were inadequate to safeguard Plaintiffs' and Class Members' Private Information, and that the risk of a data breach or theft was highly likely. PracticeMax's actions in engaging in these deceptive acts and practices were intentional, knowing and willful, and wanton and reckless with respect to the rights of Plaintiffs and Class Members.

270. Specifically, PracticeMax failed to comply with the standards outlined by the FTC and HIPAA regarding protecting PHI. PracticeMax was or should have been aware of these standards. PracticeMax's data security systems did not follow the FTC's guidelines and HIPAA's Administrative Simplification Rules. And thus, PracticeMax's systems operated below the minimum standards required.

271. Plaintiffs and Class Members were ignorant of the truth and relied on the concealed facts in providing their Private Information and incurred damages as a consequent and proximate result.

272. Plaintiffs and Class Members seek all available relief under A.R.S. §§ 44-1521, *et seq.*, including, but not limited to, compensatory damages, punitive damages, injunctive relief, and attorneys' fees and costs.

SIXTH CAUSE OF ACTION
Violations of the Illinois Consumer Fraud and Deceptive Business Practices Act
815 Ill. Comp. Stat. §§ 505/1, *et seq*.
(On behalf of Plaintiff Witkowski and the Illinois Sub-Class)

273. Plaintiff Witkowski and the Illinois Sub-Class (referred to in this Count as the "Class") repeat and re-allege each and every allegation in the Complaint as if fully set forth herein.

274. Plaintiff and the Class are "consumers" as defined in 815 Ill. Comp. Stat. § 505/1(e). Plaintiff, the Class, and Defendant are "persons" as defined in 815 Ill. Comp. Stat. § 505/1(c).

275. Defendant engaged in "trade" or "commerce," including the provision of services, as defined under 815 Ill. Comp. Stat. § 505/1(f). Defendant engages in the sale of "merchandise" (including services) as defined by 815 Ill. Comp. Stat. § 505/1(b) and (d).

276. Defendant engaged in deceptive and unfair acts and practices, misrepresentation, and the concealment and omission of material facts in connection with the sale and advertisement of its services in violation of the Illinois Consumer Fraud and Deceptive Business Practices Act ("CFA"), including: (1) failing to maintain adequate data security to keep Plaintiff's and the Class Members' sensitive PII from being stolen by cybercriminals and failing to comply with applicable state and federal laws and industry standards pertaining to data security, including the FTC Act; (2) failing to disclose or omitting materials facts to Plaintiff and the Class regarding their lack of adequate data security and inability or unwillingness to properly secure and protect the PII of Plaintiffs and the Class; (3) failing to disclose or omitting materials facts to Plaintiff and the Class about Defendant's failure to comply with the requirements of relevant federal and state laws pertaining to the privacy and security of the PII of Plaintiffs and the Class; and (4) failing to take proper action following the Data Breach to enact adequate privacy and security measures and protect Plaintiff's and the Class's PII and other personal information from further unauthorized disclosure, release, data breaches, and theft.

277. These actions also constitute deceptive and unfair acts or practices because Defendant knew the facts about its inadequate data security and failure to comply with applicable state and federal laws and industry standards would be unknown to and not easily discoverable by Plaintiff and the Class and defeat their reasonable expectations about the security of their PII.

278. Defendant intended that Plaintiff and the Class rely on its deceptive and unfair acts and practices and the concealment and omission of material facts in connection with Defendant's offering of goods and services.

279. Defendant's wrongful practices were and are injurious to the public because those practices were part of Defendant's generalized course of conduct that applied to the Class. Plaintiff and the Class have been adversely affected by Defendant's conduct and the public was and is at risk as a result thereof.

280. Defendant also violated 815 ILCS 505/2 by failing to immediately notify Plaintiff and the Class of the nature and extent of the Data Breach pursuant to the Illinois Personal Information Protection Act, 815 ILCS 530/1, *et seq*.

281. As a result of Defendant's wrongful conduct, Plaintiff and the Class were injured in that they never would have provided their PII to Defendant had they known or been told that Defendant failed to maintain sufficient security to keep their PII from being hacked and taken and misused by others.

282. As a direct and proximate result of Defendant's violations of the CFA, Plaintiff and the Class have suffered harm: (1) actual identity theft; (2) the loss of the opportunity how their PII is used; (3) the compromise, publication, and/or theft of their PII; (4) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, and/or unauthorized use of their PII; (5) 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; (6) the continued risk to their PII, 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 PII in their continued possession; and (7) 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 Class Members.

283. Pursuant to 815 Ill. Comp. Stat. § 505/10a(a), Plaintiff and the Class seek actual and compensatory damages, injunctive relief, and court costs and attorneys' fees as a result of Defendant's violations of the CFA.

SEVENTH CAUSE OF ACTION
Violations of the Tennessee Identity Theft Deterrence Act of 1999
Tenn. Code. Ann § 47-18-2101, *et seq.*
(On behalf of Plaintiff Knox and the Tennessee Sub-Class)

284. Plaintiff Knox and the Tennessee Sub-Class (referred to in this Count as the "Class") repeat and re-allege each and every allegation in the Complaint as if fully set forth herein.

285. Defendant is a business that owns or licenses computerized data that includes "personal information" as defined by Tenn. Code Ann. § 47-18-2107(a)(2) ("Personal Information").

286. Plaintiff and Tennessee Sub-Class members' Private Information that was compromised in the Data Breach includes Personal Information as covered under Tenn. Code Ann. § 47-18-2107(a)(3)(A).

287. Defendant was required to accurately notify Plaintiff and Tennessee Sub-Class members if it became aware of a breach of its data security systems that was reasonably likely to have caused unauthorized persons to acquire Plaintiff's and Tennessee Sub-Class members' Personal Information in the most expedient time possible and without unreasonable delay under Tenn. Code Ann. § 47-18-2107(b).

288. Because Defendant discovered a breach of their security systems in which unencrypted Private Information was, or is reasonably believed to have been, acquired by an unauthorized person, Defendant had an obligation to disclose the Data Breach in a timely and accurate fashion as mandated by Tenn. Code Ann. § 47-18-2107(b).

289. By failing to disclose the Data Breach in a timely and accurate manner, Defendant violated Tenn. Code Ann. § 47-18-2107(b).

290. As a direct and proximate result of Defendant's violations of Tenn. Code Ann. § 47-18-2107(b), Plaintiff and Tennessee Sub-Class members suffered damages, as described above.

291. Plaintiff and Tennessee Sub-Class members seek relief under Tenn. Code Ann. §§ 47-18-2107(h), 47-18-2104(d), and 47-18-2104(f), including actual damages and injunctive relief.

EIGHTH CAUSE OF ACTION
Violations of the Tennessee Consumer Protection Act
Tenn. Code. Ann § 47-18-101, *et seq.*
(On behalf of Plaintiff Knox and the Tennessee Sub-Class)

292. Plaintiff Knox and the Tennessee Sub-Class (referred to in this Count as the "Class") repeat and re-allege each and every allegation in the Complaint as if fully set forth herein.

293. Tenn. Code Ann. § 47-18-109(a)(1) provides that "[a]ny person who suffers an ascertainable loss of money or property, real, personal, or mixed, or any other article, commodity, or thing of value wherever situated, as a result of the use or employment by another person of an unfair or deceptive act or practice described in § 47-18-104(b) and declared to be unlawful by this part, may bring an action individually to recover actual damage."

294. Tenn. Code Ann. § 47-18-109(a)(3) further provides that "[i]f the court finds that the use or employment of the unfair or deceptive act or practice was willful or knowing violation of this part, the court may award three (3) times the actual damages sustained and may provide such other relief as it considers necessary and proper…."

295. Defendant's medical management services constitute "trade or commerce."

296. Defendant's conduct violates the Tennessee Consumer Protection Act because Defendant engaged in the deceptive acts and practices described above, which included a failure to protect Plaintiff's and the Tennessee Sub-Class's Personal Information in spite of assurances to the contrary.

297. Defendant omitted material facts concerning the steps they took (or failed to undertake) to protect Plaintiff and Tennessee Sub-Class members' Private Information, which were deceptive, false and misleading given the conduct described herein. Such conduct is inherently and materially deceptive and misleading in a material respect, which Defendant knew, or by the exercise of reasonable care, should have known, to be untrue, deceptive or misleading. Such conduct is unfair, deceptive, untrue, or misleading in that Defendant: (a) represented that its services have approval, characteristics, uses or benefits that they do not have; and (b) represented that its services are of a particular standard, quality or grade.

298. Defendant's materially misleading statements and deceptive acts and practices alleged herein were directed at the public at large.

299. Defendant's actions impact the public interest because Plaintiff and the Tennessee Sub-Class have been injured in exactly the same way as thousands of others as a result of and pursuant to Defendant's generalized course of deception as described herein.

300. Defendant's acts and practices described above were likely to mislead a reasonable consumer acting reasonably under the circumstances.

301. Defendant's misrepresentations, misleading statements and omissions were materially misleading to Plaintiff and members of the Tennessee Sub-Class.

302. Defendant's violation of Tenn. Code Ann. § 47-18-104 was willful and knowing. As described above, at all relevant times, Defendant among other things, knew that its policies and procedures for the protection of Plaintiff's and the Tennessee Sub-Class's Private Information were inadequate to protect that Private Information.

Nonetheless, Defendant continued to solicit and process Private Information in the United States in order to increase its own profits.

303. Had Plaintiff and the members of the Tennessee Sub-Class known of Defendant's misrepresentations, misleading statements and omissions about their use of Private Information, they would not have permitted the use of Defendant's services and given Defendant or Defendant's clients their Private Information.

304. As a direct and proximate result of Defendant's conduct in violation of Tenn. Code Ann. § 47-18-104, Plaintiff and the members of the Tennessee Sub-Class have been injured in amounts to be proven at trial.

305. As a result, pursuant to Tenn. Code Ann. §§ 47-18-104 and 47-18-109, Plaintiff and the Tennessee Sub-Class are entitled to damages in an amount to be determined at trial. Plaintiff also properly asks that such damages be trebled based on Defendant's knowledge and/or intention with respect to the Breach.

306. Plaintiff also seeks injunctive relief, including a robust, state of the art notice program for the wide dissemination of a factually accurate statement on the actual state of Defendant's Private Information storage and the implementation of a corrective advertising campaign by Defendant.

307. Additionally, pursuant to Tenn. Code Ann. § 47-18-109, Plaintiff and the Tennessee Sub-Class make claims for attorneys' fees and costs.

PRAYER FOR RELIEF

WHEREFORE Plaintiffs, on behalf of themselves and all others similarly situated, request the following relief:

A. An Order certifying this action as a class action and appointing Plaintiffs as Class representatives and the undersigned as Class counsel;

B. A mandatory injunction directing PracticeMax to adequately safeguard the Private Information of Plaintiffs and the Class hereinafter by implementing

improved security procedures and measures, including but not limited to an Order:

i. prohibiting PracticeMax from engaging in the wrongful and unlawful acts described herein;

ii. requiring PracticeMax to protect, including through encryption, all data collected through the course of business in accordance with all applicable regulations, industry standards, and federal, state or local laws;

iii. requiring PracticeMax to delete and purge the Private Information of Plaintiffs and Class Members unless PracticeMax can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiffs and Class Members;

iv. requiring PracticeMax to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of Plaintiffs' and Class Members' Private Information;

v. requiring PracticeMax to engage independent third-party security auditors and internal personnel to run automated security monitoring, simulated attacks, penetration tests, and audits on PracticeMax's systems on a periodic basis;

vi. prohibiting PracticeMax from maintaining Plaintiffs' and Class Members' Private Information on a cloud-based database;

vii. requiring PracticeMax to segment data by creating firewalls and access controls so that, if one area of PracticeMax's network is compromised, hackers cannot gain access to other portions of PracticeMax's systems;

viii. requiring PracticeMax to conduct regular database scanning and securing checks;

ix. requiring PracticeMax to monitor ingress and egress of all network traffic;

x. requiring PracticeMax to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon the employees' respective responsibilities with handling Private Information, as well as protecting the Private Information of Plaintiffs and Class Members;

xi. requiring PracticeMax to implement a system of tests to assess its respective employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees' compliance with PracticeMax's policies, programs, and systems for protecting personal identifying information;

xii. requiring PracticeMax to implement, maintain, review, and revise as necessary a threat management program to appropriately monitor PracticeMax's networks for internal and external threats, and assess whether monitoring tools are properly configured, tested, and updated;

xiii. requiring PracticeMax to meaningfully educate all Class Members about the threats that they face because of the loss of its confidential personal identifying information to third parties, as well as the steps affected individuals must take to protect themselves; and

xiv. requiring PracticeMax to provide adequate credit monitoring to all Class Members.

C. A mandatory injunction requiring that PracticeMax provide notice to each member of the Class relating to the full nature and extent of the Data Breach and the disclosure of Private Information to unauthorized persons;

D. Enjoining PracticeMax from further deceptive practices and making untrue statements about the Data Breach and the stolen Private Information;

E. An award of damages, including actual, nominal, consequential damages, and punitive, as allowed by law in an amount to be determined;

F. An award of attorneys' fees, costs, and litigation expenses, as allowed by law;

G. An award of pre- and post-judgment interest, costs, attorneys' fees, expenses, and interest as permitted by law;

H. Granting the Plaintiffs and the Class leave to amend this complaint to conform to the evidence produced at trial;

I. For all other Orders, findings, and determinations identified and sought in this Complaint; and

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

JURY TRIAL DEMANDED

Under Federal Rule of Civil Procedure 38(b), Plaintiffs demand a trial by jury for any and all issues in this action so triable as of right.

Dated: October 31, 2022

Respectfully Submitted,

/s/Elaine A. Ryan

AUER RYAN, P.C.
Elaine A. Ryan (AZ Bar #012870)
Colleen M. Auer (AZ Bar #014637)
20987 N. John Wayne Parkway, #B104-374
Maricopa, AZ 85139
T: (520) 705-7332
eryan@auer-ryan.com
cauer@auer-ryan.com

PEREZ LAW GROUP, PLLC
Cristina Perez Hesano (#027023)
7508 N. 59th Avenue
Glendale, AZ 85301
T: (602) 730-7100
F: (623) 235-6173
cperez@perezlawgroup.com

MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN, PLLC
Gary M. Klinger *(Pro Hac Vice Forthcoming)*
221 West Monroe Street, Suite 2100
Chicago, IL 60606
T: 866.252.0878
gklinger@milberg.com

MARKOVITS, STOCK & DEMARCO, LLC
Terence R. Coates *(Pro Hac Vice Forthcoming)*
Jonathan T. Deters *(Pro Hac Vice Forthcoming)*
119 E. Court Street, Suite 530
Cincinnati, OH 45202
T: 513.651.3700
F: 513.665.0219
tcoates@msdlegal.com
jdeters@msdlegal.com

TURKE & STRAUSS LLP
Samuel J. Strauss (*Pro Hac Vice Forthcoming)*
Raina C. Borrelli (*admitted Pro Hac Vice*)
613 Williamson St., Suite 201
Madison, WI 53703
T: (608) 237-1775
F: (608) 509-4423
sam@turkestrauss.com
raina@turkestrauss.com

MORGAN & MORGAN COMPLEX LITIGATION DIVISION
John A. Yanchunis (*Pro Hac Vice Forthcoming)*
Ryan Maxey (*Pro Hac Vice Forthcoming)*
Ra O. Amen (*Pro Hac Vice Forthcoming)*
201 N. Franklin Street, 7th Floor
Tampa, Florida 33602
T: (813) 223-5505
jyanchunis@ForThePeople.com

rmaxey@ForThePeople.com
ramen@ForThePeople.com

THE CONSUMER PROTECTION FIRM
William 'Billy' Peerce Howard (*Pro Hac Vice Forthcoming)*
401 E. Jackson St., Suite 2340
Tampa, Florida 33602
T: (813) 500-1500
F: (813) 435-2369
Billy@TheConsumerProtectionFirm.com

FEDERMAN & SHERWOOD
William B. Federman (admitted *Pro Hac Vice)*
10205 N. Pennsylvania Ave.
Oklahoma City, OK 73120
T: (405) 235-1560
wbf@federmanlaw.com

MURPHY LAW FIRM
A. Brooke Murphy (admitted *Pro Hac Vice)*
4116 Will Rogers Pkwy, Suite 700
Oklahoma City, OK 73108
T: (405) 389-4989
abm@murphylegalfirm.com

Counsel for Plaintiffs and the Classes

CERTIFICATE OF SERVICE

I HEREBY CERTIFY that on this 31st day of October, 2022, I electronically filed the foregoing with the Clerk of the Court using the CM/ECF system which will send notification of such filing to the e-mail addresses denoted on the Electronic Mail notice list.

/s/ Colleen M. Auer