UNITED STATES DISTRICT COURT
DISTRICT OF MASSACHUSETTS
SPRINGFIELD DIVISION

JOSE MORAES, on behalf of himself and all others similarly situated, Plaintiff, v. **WELLFLEET GROUP, LLC,** Defendant.	Case No. **JURY TRIAL DEMANDED**

CLASS ACTION COMPLAINT

Plaintiff Jose Moraes ("Plaintiff"), individually and on behalf of all similarly situated persons, allege the following against Wellfleet Group, LLC ("Wellfleet" or "Defendant") based upon personal knowledge with respect to himself and on information and belief derived from, among other things, investigation by Plaintiff's counsel and review of public documents as to all other matters:

I. INTRODUCTION

1. Plaintiff brings this class action against Wellfleet for its failure to properly secure and safeguard Plaintiff's and other similarly situated individuals' personally identifiable information ("PII") and protected health information ("PHI"), including full name, mailing address, insurance group/policy number, school ID number, and medical/health information (the "Private Information"), from unauthorized, public disclosure.

2. Wellfleet, which is based in Springfield, Massachusetts, is an accident and health insurance company that serves students in higher education markets nationwide.

3. On or about, October 14, 2024 Wellfleet filed official notice of a data security incident with the Office of the Texas Attorney General, as well as with the U.S. Department of Health and Human Services Office for Civil Rights. Under state and federal law, organizations must report breaches involving PHI within at least sixty (60) days.

4. On or about October 14, 2024, Wellfleet also sent out notice letters to individuals whose information was implicated in the incident (the "Notice").

5. Based on the Notice sent to Plaintiff and "Class Members" (defined below), unusual activity was detected on its website and, in response, Defendant initiated an investigation that revealed a misconfiguration on the website allowing students' Private Information to be "accessible online via a common Internet search engine[,]" which then enabled "web crawlers" to "scrape the [Private Information] and index [it]" (the "Data Incident").

6. Unfortunately for Plaintiff and other similarly situated individuals, the Private Information revealed in the Data Incident contained highly sensitive health data, representing a gold mine for data thieves.

7. Armed with such Private Information (and a head start), data thieves can commit a variety of crimes, including the use of such information to obtain medical services in Class Members' names.

8. There has been no assurance offered by Wellfleet that it has adequately enhanced its data security practices sufficient to avoid a similar incident from occurring in the future.

9. Therefore, Plaintiff and Class Members have suffered and are at an imminent, immediate, and continuing increased risk of suffering, ascertainable losses in the form of harm from identity theft and other fraudulent misuse of their Private Information, the loss of the benefit of their bargain, out-of-pocket expenses incurred to remedy or mitigate the effects of the

Data Incident, and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Incident.

10. Plaintiff brings this class action lawsuit to address Wellfleet's inadequate safeguarding of Class Members' Private Information that it collected and maintained.

11. The potential for improper disclosure and theft of Plaintiff's and Class Members' Private Information was a known risk to Wellfleet, and thus Wellfleet was on notice that failing to take necessary steps to secure the Private Information left it vulnerable.

12. Upon information and belief, Wellfleet failed to properly implement security practices with regard to its website that housed the Private Information. Had Wellfleet properly monitored its networks, it would have discovered the Breach sooner.

13. Plaintiff's and Class Members' identities are now at risk because of Wellfleet's negligent conduct as the Private Information that Wellfleet collected and maintained is now in the hands of data thieves and other unauthorized third parties.

14. Plaintiff seeks to remedy these harms on behalf of himself and all similarly situated individuals whose Private Information was accessible during the Data Incident.

15. Accordingly, Plaintiff, on behalf of himself and the Class, asserts claims for negligence, negligence *per se*, breach of implied contract, unjust enrichment, and declaratory judgment this Court deems just and proper.

II. PARTIES

16. Plaintiff Jose Moraes is, and at all times mentioned herein was, an individual citizen of the State of Oklahoma.

17. Defendant Wellfleet is an insurance company incorporated in Massachusetts with its principal place of business at 1500 Main St, Springfield, MA 01103 in Hampden County.

III. JURISDICTION AND VENUE

18. The Court has subject matter jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). The amount in controversy exceeds $5 million, exclusive of interest and costs. Upon information and belief, the number of class members is over 100, many of whom have different citizenship from Wellfleet. Thus, minimal diversity exists under 28 U.S.C. § 1332(d)(2)(A).

19. This Court has jurisdiction over Wellfleet because Wellfleet operates in and/or is incorporated in this District.

20. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(a)(1) because a substantial part of the events giving rise to this action occurred in this District and Wellfleet has harmed Class Members residing in this District.

IV. FACTUAL ALLEGATIONS

A. Wellfleet's Business and Collection of Plaintiff's and Class Members' Private Information

21. Wellfleet, a Berkshire Hathaway company, is a health and accident insurance company focusing on students of higher education. Founded in 1993 as Consolidated Health Plans (CHP), Wellfleet is one of the nation's leading providers of health and accident insurance products to the higher education market. Wellfleet employs more than 237 people and generates approximately $86 million in annual revenue.

22. As a condition of receiving insurance services, Wellfleet requires that its customers entrust it with highly sensitive personal and health information. In the ordinary course of receiving service from Wellfleet, Plaintiff and Class Members were required to provide their Private Information to Defendant.

23. In its Notice of Privacy Practices, Wellfleet promises its customers that it is "committed to protecting medical information about you" and says that it is required by law to "[e]nsure that information that identifies you is kept private."[1] Wellfleet also describes in its Privacy Policy the limited specific instances when it shares customer health information."[2]

24. Thus, due to the highly sensitive and personal nature of the information Wellfleet acquires and stores with respect to its customers, Wellfleet, upon information and belief, promises to, among other things: keep customers' Private Information private; comply with industry standards related to data security and the maintenance of its customers' Private Information; inform its customers of its legal duties relating to data security and comply with all federal and state laws protecting customers' Private Information; only use and release customers' Private Information for reasons that relate to the services it provides; and provide adequate notice to customers if their Private Information is disclosed without authorization.

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

26. Plaintiff and Class Members relied on Wellfleet to keep their Private Information confidential and securely maintained and to only make authorized disclosures of this Information, which Defendant ultimately failed to do.

[1] https://wellfleetinsurance.com/privacy-policy/ (last visited on Oct. 24, 2024).

[2] *Id.*

B. The Data Incident and Defendant's Inadequate Notice to Plaintiff and Class Members

27. According to Defendant's Notice, it learned of the unauthorized disclosure of student health information via a misconfiguration in its website on August 1, 2024.

28. On or about October 14, 2024, roughly two (2) months after Wellfleet learned that the Class's Private Information was disclosed, Wellfleet finally began to notify individuals that its investigation determined that their Private Information was involved.

29. Wellfleet delivered Notice of Data Security Incident letters to Plaintiff and Class Members, alerting them that their highly sensitive Private Information had been exposed.

30. Omitted from the Notice are crucial details like the root cause of the Data Incident, the vulnerabilities exploited, and the remedial measures undertaken to ensure such a breach does not occur again. To date, these critical facts have not been explained or clarified to Plaintiff and Class Members, who retain a vested interest in ensuring that their Private Information is protected.

31. Thus, Wellfleet's purported disclosure amounts to no real disclosure at all, as it fails to inform Plaintiff and Class Members of the Data Incident's critical facts with any degree of specificity. Without these details, Plaintiff's and Class Members' ability to mitigate the harms resulting from the Data Incident was and is severely diminished.

32. In addition, the Notice offers no substantive steps to help victims like Plaintiff and Class Members to protect themselves other than providing two (2) years of credit monitoring – an offer that is woefully inadequate considering the lifelong increased risk of fraud and identity theft Plaintiff and Class Members now face as a result of the Data Incident

33. Wellfleet had obligations created by contract, industry standards, common law, and representations made to Plaintiff and Class Members to keep Plaintiff's and Class Members' Private Information confidential and to protect it from unauthorized access and disclosure.

34. Plaintiff and Class Members provided their Private Information to Wellfleet with the reasonable expectation and mutual understanding that Wellfleet would comply with its obligations to keep such Information confidential and secure from unauthorized access and to provide timely notice of any security breaches.

35. Wellfleet's data security obligations were particularly important given the substantial increase in cyberattacks in recent years.

36. Wellfleet knew or should have known that its electronic records would be targeted by cybercriminals.

C. Wellfleet Failed to Comply with HIPAA

37. Title II of HIPAA contains what are known as the Administration Simplification provisions. *See* 42 U.S.C. §§ 1301, *et seq*. These provisions require that HHS create rules to streamline the standards for handling PHI similar to the data Defendant left unguarded and vulnerable to attack. The HHS has subsequently promulgated five rules under authority of the Administrative Simplification provisions of HIPAA.

38. Wellfleet's Data Incident resulted from a combination of insufficiencies that indicate Wellfleet failed to comply with safeguards mandated by HIPAA regulations and industry standards. First, it can be inferred from Wellfleet's Data Incident that Wellfleet either failed to implement, or inadequately implemented, information security policies or procedures to protect Plaintiff's and Class Members' PHI.

39. Plaintiff's and Class Members' Private Information compromised in the Data Incident included "protected health information" as defined by CFR § 160.103.

40. 45 CFR § 164.402 defines "breach" as "the acquisition, access, use, or disclosure of protected health information in a manner not permitted under subpart E of this part which compromises the security or privacy of the protected health information."

41. 45 CFR § 164.402 defines "unsecured protected health information" as "protected health information that is not rendered unusable, unreadable, or indecipherable to unauthorized persons through the use of a technology or methodology specified by the [HHS] Secretary[.]"

42. Plaintiff's and Class Members' Private Information included "unsecured protected health information" as defined by 45 CFR § 164.402.

43. Plaintiff's and Class Members' unsecured PHI was acquired, accessed, used, and/or disclosed in a manner not permitted under 45 CFR, Subpart E, as a result of the Data Incident.

44. Based upon Defendant's Notice to Plaintiff and Class Members, Wellfleet reasonably believes that Plaintiff's and Class Members' unsecured PHI has been acquired, accessed, used, and/or disclosed in a manner not permitted under 45 CFR, Subpart E, as a result of the Data Incident.

45. Plaintiff's and Class Members' unsecured PHI that was acquired, accessed, used, and/or disclosed in a manner not permitted under 45 CFR, Subpart E as a result of the Data Incident was not rendered unusable, unreadable, or indecipherable to unauthorized persons.

46. Wellfleet reasonably believes that Plaintiff's and Class Members' unsecured PHI that was acquired, accessed, used, and/or disclosed in a manner not permitted under 45 CFR,

Subpart E as a result of the Data Incident was not rendered unusable, unreadable, or indecipherable to unauthorized persons.

47. Plaintiff's and Class Members' unsecured PHI that was acquired, accessed, used, and/or disclosed in a manner not permitted under 45 CFR, Subpart E as a result of the Data Incident, and which was not rendered unusable, unreadable, or indecipherable to unauthorized persons, was viewed by unauthorized persons.

48. Plaintiff's and Class Members' unsecured PHI was viewed by unauthorized persons in a manner not permitted under 45 CFR, Subpart E as a result of the Data Incident.

49. Wellfleet reasonably believes that Plaintiff's and Class Members' unsecured PHI was viewed by unauthorized persons in a manner not permitted under 45 CFR, Subpart E as a result of the Data Incident.

50. It is reasonable to infer that Plaintiff's and Class Members' unsecured PHI that was acquired, accessed, used, and/or disclosed in a manner not permitted under 45 CFR, Subpart E as a result of the Data Incident, and which was not rendered unusable, unreadable, or indecipherable to unauthorized persons, was viewed by unauthorized persons.

51. It should be rebuttably presumed that unsecured PHI acquired, accessed, used, and/or disclosed in a manner not permitted under 45 CFR, Subpart E, and which was not rendered unusable, unreadable, or indecipherable to unauthorized persons, was viewed by unauthorized persons.

52. After receiving notice that they were victims of the Data Incident (which required the filing of a data breach report in accordance with 45 CFR § 164.408(a)), it is reasonable for recipients of that notice, including Plaintiff and Class Members in this case, to believe that future

harm (including medical identity theft) is real and imminent, and to take steps necessary to mitigate that risk of future harm.

53. In addition, Wellfleet's Data Incident could have been prevented if Wellfleet had implemented HIPAA mandated, industry standard policies and procedures for securely disposing of PHI when it was no longer necessary and/or had honored its obligations to its customers.

54. Wellfleet's security failures also include, but are not limited to:

a. Failing to maintain an adequate data security system to prevent data loss;

b. Failing to mitigate the risks of a data incident and disclosure of health data;

c. Failing to ensure the confidentiality and integrity of electronic protected health information Wellfleet creates, receives, maintains, and transmits in violation of 45 CFR 164.306(a)(1);

d. Failing to implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights in violation of 45 CFR 164.312(a)(1);

e. Failing to implement policies and procedures to prevent, detect, contain, and correct security violations in violation of 45 CFR 164.308(a)(1);

f. Failing to identify and respond to suspected or known security incidents;

g. Failing to mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity, in violation of 45 CFR 164.308(a)(6)(ii);

h. Failing to protect against any reasonably-anticipated threats or hazards to the security or integrity of electronic protected health information, in violation of 45 CFR 164.306(a)(2);

i. Failing to protect against any reasonably anticipated uses or disclosures of electronic protected health information that are not permitted under the privacy rules regarding individually identifiable health information, in violation of 45 CFR 164.306(a)(3);

j. Failing to ensure compliance with HIPAA security standard rules by Defendant's workforce, in violation of 45 CFR 164.306(a)(94); and

k. Impermissibly and improperly using and disclosing protected health information that is and remains accessible to unauthorized persons, in violation of 45 CFR 164.502, *et seq.*

55. Because Wellfleet has failed to comply with HIPAA, while monetary relief may cure some of Plaintiff's and Class Members' injuries, injunctive relief is also necessary to ensure Wellfleet's approach to information security is adequate and appropriate going forward. Wellfleet still maintains the PHI and other highly sensitive PII of its current and former customers, including Plaintiff and Class Members. Without the supervision of the Court through injunctive relief, Plaintiff's and Class Members' Private Information remains at risk of subsequent data breaches.

D. Wellfleet Failed to Comply with FTC Guidelines

56. The Federal Trade Commission ("FTC") has promulgated numerous guides for businesses which highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision making. Indeed, the FTC has concluded that a company's failure to maintain reasonable and appropriate data security for consumers' sensitive personal information is an "unfair practice" in

violation of Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. *See, e.g., FTC v. Wyndham Worldwide Corp.*, 799 F.3d 236 (3d Cir. 2015).

57. In October 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established cybersecurity guidelines for businesses.[3] . The guidelines note that businesses should protect the personal customer information that they keep, properly dispose of personal information that is no longer needed, encrypt information stored on computer networks, understand their network's vulnerabilities, and implement policies to correct any security problems. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs, monitor all incoming traffic for activity indicating someone is attempting to hack into the system, watch for large amounts of data being transmitted from the system, and have a response plan ready in the event of a breach.

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

59. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data by 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 FTC Act, 15 U.S.C. § 45 *et seq*. Orders

[3] *Protecting Personal Information: A Guide for Business*, FEDERAL TRADE COMMISSION (October 2016), *available at* https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last visited on Oct. 24, 2024).

resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

60. Such FTC enforcement actions include those against businesses that fail to adequately protect customer data, like Wellfleet here. *See, e.g.*, *In the Matter of LabMD, Inc*., 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.").

61. Section 5 of the FTC Act, 15 U.S.C. § 45, prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses like Wellfleet of failing to use reasonable measures to protect Private Information they collect and maintain from customers. The FTC publications and orders described above also form part of the basis of Wellfleet's duty in this regard.

62. The FTC has also recognized that personal 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. The larger the data set, the greater potential for analysis and profit."[4]

63. As evidenced by the Data Incident, Wellfleet failed to properly implement basic data security practices. Wellfleet's failure to employ reasonable and appropriate measures to protect against unauthorized access to Plaintiff's and Class Members' Private Information constitutes an unfair act or practice prohibited by Section 5 of the FTCA.

[4] FTC Commissioner Pamela Jones Harbour, *Remarks Before FTC Exploring Privacy Roundtable* (Dec. 7, 2009), *transcript available at* https://www.ftc.gov/sites/default/files/documents/public_statements/remarks-ftc-exploring-privacy-roundtable/091207privacyroundtable.pdf (last visited on Oct. 24, 2024).

64. Wellfleet was at all times fully aware of its obligation to protect the Private Information of its customers yet failed to comply with such obligations. Defendant was also aware of the significant repercussions that would result from its failure to do so.

E. Wellfleet Failed to Comply with Industry Standards

65. As noted above, experts studying cybersecurity routinely identify businesses as being particularly vulnerable to cyberattacks because of the value of the Private Information which they collect and maintain.

66. The Center for Internet Security's (CIS) Critical Security Controls (CSC) recommends certain best practices to adequately secure data and prevent cybersecurity attacks, including Critical Security Controls of Inventory and Control of Enterprise Assets, Inventory and Control of Software Assets, Data Protection, Secure Configuration of Enterprise Assets and Software, Account Management, Access Control Management, Continuous Vulnerability Management, Audit Log Management, Email and Web Browser Protections, Malware Defenses, Data Recovery, Network Infrastructure Management, Network Monitoring and Defense, Security Awareness and Skills Training, Service Provider Management, Application Software Security, Incident Response Management, and Penetration Testing.[5]

67. The National Institute of Standards and Technology ("NIST") also recommends certain practices to safeguard systems, such as the following:

a. Control who logs on to your network and uses your computers and other devices.
b. Use security software to protect data.
c. Encrypt sensitive data, at rest and in transit.
d. Conduct regular backups of data.
e. Update security software regularly, automating those updates if possible.

[5] *The 18 CIS Critical Security Controls*, CENTER FOR INTERNET SECURITY, https://www.cisecurity.org/controls/cis-controls-list (last visited on Oct. 24, 2024).

f. Have formal policies for safely disposing of electronic files and old devices.
g. Train everyone who uses your computers, devices, and network about cybersecurity. You can help employees understand their personal risk in addition to their crucial role in the workplace.

68. Further still, the United States Cybersecurity and Infrastructure Security Agency ("CISA") makes specific recommendations to organizations to guard against cybersecurity attacks, including (a) reducing the likelihood of a damaging cyber intrusion by validating that "remote access to the organization's network and privileged or administrative access requires multi-factor authentication, [e]nsur[ing] that software is up to date, prioritizing updates that address known exploited vulnerabilities identified by CISA[,] [c]onfirm[ing] that the organization's IT personnel have disabled all ports and protocols that are not essential for business purposes," and other steps; (b) taking steps to quickly detect a potential intrusion, including "[e]nsur[ing] that cybersecurity/IT personnel are focused on identifying and quickly assessing any unexpected or unusual network behavior [and] [e]nabl[ing] logging in order to better investigate issues or events[;] [c]onfirm[ing] that the organization's entire network is protected by antivirus/antimalware software and that signatures in these tools are updated," and (c) "[e]nsur[ing] that the organization is prepared to respond if an intrusion occurs," and other steps.[6]

69. Defendant failed to implement industry-standard cybersecurity measures, including by failing to meet the minimum standards of both the NIST Cybersecurity Framework Version 2.0 (including PR.AA-01, PR.AA.-02, PR.AA-03, PR.AA-04, PR.AA-05, PR.AT-01, PR.DS-01, PR-DS-02, PR.DS-10, PR.PS-01, PR.PS-02, PR.PS-05, PR.IR-01, DE.CM-01, DE.CM-03,

[6] *Shields Up: Guidance for Organizations*, CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY, https://www.cisa.gov/shields-guidance-organizations (last visited Oct. 24, 2024).

DE.CM-06, DE.CM-09, and RS.CO-04) and the Center for Internet Security's Critical Security Controls (CIS CSC), which are established frameworks for reasonable cybersecurity readiness, and by failing to comply with other industry standards for protecting Plaintiff's and Class Members' Private Information, resulting in the Data Incident.

F. Wellfleet Breached its Duty to Safeguard Plaintiff's and Class Members' Private Information

70. In addition to its obligations under federal and state laws, Wellfleet owed a duty to Plaintiff and Class Members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the Private Information in its possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons. Wellfleet owed a duty to Plaintiff and Class Members to provide reasonable security, including consistency with industry standards and requirements, and to ensure that its computer systems, networks, and protocols adequately protected the Private Information of Class Members

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

a. Failing to adequately protect the Private Information in its possession;

b. Failing to properly monitor its own data security systems, including website, for existing weaknesses and misconfigurations;

c. Failing to sufficiently train its employees regarding the proper handling of Private Information;

d. Failing to fully comply with FTC guidelines for cybersecurity in violation of the FTCA;

e. Failing to adhere to HIPAA and industry standards for cybersecurity as discussed above; and

f. Otherwise breaching its duties and obligations to protect Plaintiff's and Class Members' Private Information.

72. Wellfleet negligently and unlawfully failed to safeguard Plaintiff's and Class Members' Private Information by allowing the disclosure of unsecured and unencrypted Private Information to unauthorized third-parties.

73. Had Wellfleet remedied the deficiencies in its information storage and security systems, followed industry guidelines, and adopted security measures recommended by experts in the field, it could have prevented the unauthorized disclosure of Plaintiff's and Class Members' confidential Private Information.

74. Accordingly, Plaintiff's and Class Members' lives were severely disrupted. What's more, they have been harmed as a result of the Data Incident and now face an increased risk of future harm that includes, but is not limited to, fraud and identity theft. Plaintiff and Class Members also lost the benefit of the bargain they made with Wellfleet.

G. Plaintiff and Class Members are at a Significantly Increased and Substantial Risk of Fraud and Identity Theft as a Result of the Data Incident.

75. The FTC hosted a workshop to discuss "informational injuries," which are injuries that consumers like Plaintiff and Class Members suffer from privacy and security incidents such as data breaches or unauthorized disclosure of data.[7] Exposure of highly sensitive personal information that a consumer wishes to keep private may cause harm to the consumer, such as the ability to obtain or keep employment. Consumers' loss of trust in e-commerce also

[7] *FTC Information Injury Workshop, BE and BCP Staff Perspective*, Federal Trade Commission, (October 2018), *available at* https://www.ftc.gov/system/files/documents/reports/ftc-informational-injury-workshop-be-bcp-staff-perspective/informational_injury_workshop_staff_report_-_oct_2018_0.pdf (last visited on Oct. 24, 2024).

deprives them of the benefits provided by the full range of goods and services available which can have negative impacts on daily life.

76. Any victim of an incident like Defendant's Data Incident is exposed to serious ramifications regardless of the nature of the data that was disclosed. Indeed, the reason why criminals search for and steal such information is to monetize it. They do this by selling the information on the black market to identity thieves who desire to extort and harass victims or to take over victims' identities in order to engage in illegal financial transactions under the victims' names.

77. Because a person's identity is akin to a puzzle, the more accurate pieces of data an identity thief obtains about a person, the easier it is for the thief to take on the victim's identity or to otherwise harass or track the victim. For example, armed with just a name and date of birth, a data thief can utilize a hacking technique referred to as "social engineering" to obtain even more information about a victim's identity, such as a person's login credentials or Social Security number. Social engineering is a form of hacking whereby a data thief uses previously acquired information to manipulate individuals into disclosing additional confidential or personal information through means such as spam phone calls and text messages or phishing emails.

78. In fact, as technology advances, computer programs may scan the Internet with a wider scope to create a mosaic of information that may be used to link compromised information to an individual in ways that were not previously possible. This is known as the "mosaic effect." Names and dates of birth, combined with contact information like telephone numbers and email addresses, are very valuable to hackers and identity thieves as it allows them to access users' other accounts.

79. Thus, even if certain information was not purportedly involved in the Data Incident, the unauthorized parties could use Plaintiff's and Class Members' Private Information to access accounts, including, but not limited to, email accounts, medical accounts, insurance accounts, and/or financial accounts, to engage in a wide variety of fraudulent activity against Plaintiff and Class Members.

80. One such example of how malicious actors may compile Private Information is through the development of "Fullz" packages.

81. Cybercriminals can cross-reference two sources of the Private Information compromised in the Data Incident 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.

82. The development of "Fullz" packages means that the stolen Private Information from the Data Incident can easily be used to link and identify it to Plaintiff's and the proposed Class's phone numbers, email addresses, and other sources and identifiers. In other words, even if certain information such as emails, phone numbers, or credit card or financial account numbers may not be included in the Private Information stolen in the Data Incident, 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.

83. For these reasons, the FTC recommends that identity theft victims take several time-consuming steps to protect their personal and financial information after a data incident like this one, including contacting one of the credit bureaus to place a fraud alert on their account (and an extended fraud alert that lasts for 7 years if someone steals the victim's identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their

accounts, placing a freeze on their credit, and correcting their credit reports.[8] However, these steps do not guarantee protection from identity theft but can only mitigate identity theft's long-lasting negative impacts.

84. The Identity Theft Resource Center documents the multitude of harms caused by fraudulent use of PII in its 2023 Consumer Impact Report.[9] After interviewing over 14,000 identity crime victims, researchers found that as a result of the criminal misuse of their PII:

- 77-percent experienced financial-related problems;
- 29-percent experienced financial losses exceeding $10,000;
- 40-percent were unable to pay bills;
- 28-percent were turned down for credit or loans;
- 37-percent became indebted;
- 87-percent experienced feelings of anxiety;
- 67-percent experienced difficulty sleeping; and
- 51-percent suffered from panic of anxiety attacks.[10]

85. PHI is also especially valuable to identity thieves. As the FTC recognizes, identity thieves can use PHI to commit an array of crimes, including identity theft and medical and financial fraud.[11]

86. Indeed, a robust cyber black market exists in which criminals openly post stolen PHI on multiple underground Internet websites, commonly referred to as the dark web.

87. While credit card information and associated PII can sell for as little as $1-$2 on the black market, PHI can sell for as much as $363 according to the Infosec Institute.[12]

---

[8] *See IdentityTheft.gov*, Federal Trade Commission, *available at* https://www.identitytheft.gov/Steps (last visited Oct. 24, 2024).

[9] *2023 Consumer Impact Report* (Jan. 2024), IDENTITY THEFT RESOURCE CENTER, *available online at*: https://www.idtheftcenter.org/wp-content/uploads/2023/08/ITRC_2023-Consumer-Impact-Report_Final-1.pdf (last visited on Oct. 24, 2024).

[10] *Id* at pp 21-25.

[11] Federal Trade Commission, *Warning Signs of Identity Theft, available at*: https://consumer.ftc.gov/articles/what-know-about-identity-theft (last visited on Oct. 24, 2024).

88. PHI is particularly valuable because criminals can use it to target victims with frauds and scams that take advantage of the victim's medical conditions or victim settlements. It can be used to create fake insurance claims, allowing for the purchase and resale of medical equipment, or gain access to prescriptions for illegal use or resale.

89. Medical identity theft can result in inaccuracies in medical records and costly false claims. It can also have life-threatening consequences. If a victim's health information is mixed with other records, it can lead to misdiagnosis or mistreatment. "Medical identity theft is a growing and dangerous crime that leaves its victims with little to no recourse for recovery," reported Pam Dixon, executive director of World Privacy Forum. "Victims often experience financial repercussions and worse yet, they frequently discover erroneous information has been added to their personal medical files due to the thief's activities."[13]

90. The ramifications of Wellfleet's failure to keep Plaintiff's and Class Members' Private Information secure are long lasting and severe. Once it is stolen, fraudulent use of such and damage to victims may continue for years.

91. The value of both PII and PHI is axiomatic. The value of "big data" in corporate America is astronomical. The fact that identity thieves attempt to steal identities notwithstanding possible heavy prison sentences illustrates beyond a doubt that the Private Information compromised here has considerable market value.

92. It must also be noted that there may be a substantial time lag between when harm occurs and when it is discovered, and also between when PII and/or PHI is stolen and when it is

---

[12] *Data Breaches: In the Healthcare Sector*, CENTER FOR INTERNET SECURITY, *available at*: https://www.cisecurity.org/insights/blog/data-breaches-in-the-healthcare-sector (last visited on Oct. 24, 2024).

[13] Michael Ollove, "*The Rise of Medical Identity Theft in Healthcare*," KAISER HEALTH NEWS (Feb. 7, 2014), *available at*: https://kffhealthnews.org/news/rise-of-indentity-theft/ (last visited on Oct. 24, 2024).

misused. According to the U.S. Government Accountability Office, which conducted a study regarding data incidents such as this:[14]

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.

93. PII and PHI are such valuable commodities to identity thieves that once the information has been compromised, criminals often trade the information on the dark web for years.

94. As a result, Plaintiff and Class Members are at an increased risk of fraud and identity theft, including medical identity theft, for many years into the future. Thus, Plaintiff and Class Members have no choice but to vigilantly monitor their accounts for many years to come.

H. Plaintiff's and Class Members' Damages

Plaintiff Moraes' Experience

95. Defendant required Plaintiff Moraes provide it with substantial amounts of his Private Information, including PHI, in exchange for receiving health insurance and other related services from Defendant.

96. On or about October 11, 2024, Plaintiff Moraes received the Notice, which told him that his Private Information had been impacted as a result of the Data Incident. The Notice informed him that the Private Information accessed through the Data Incident included his full

[14] *Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown*, U.S. GOVERNMENT ACCOUNTABILITY OFFICE (June 2007), *available at* https://www.gao.gov/assets/gao-07-737.pdf (last visited on Oct. 24, 2024).

name, mailing address, insurance group/policy number, school ID number, and medical/health information."

97. The Notice offered Plaintiff Moraes only two (2) years of credit monitoring services – an insufficient amount of time given that Plaintiff will now experience a lifetime of increased risk of identity theft, including but not limited to, potential medical fraud.

98. Plaintiff Moraes suffered actual injury in the form of time spent dealing with the Data Incident and the increased risk of fraud resulting from the Data Incident and/or monitoring his accounts for fraud.

99. Plaintiff Moraes would not have provided his Private Information to Defendant had Defendant timely disclosed that its systems, including its website, lacked adequate computer and data security practices to safeguard the highly sensitive personal and health information in its possession and control.

100. Plaintiff Moraes suffered actual injury in the form of having his Private Information shared with unauthorized third parties as a result of the Data Incident.

101. Plaintiff Moraes suffered actual injury in the form of damages to and diminution in the value of his personal, health, and financial information – a form of intangible property that Plaintiff entrusted to Defendant for the purpose of receiving healthcare insurance services from Defendant and which was compromised in, and as a result of, the Data Incident.

102. Plaintiff Moraes suffered imminent and impending injury arising from the substantially increased risk of future fraud, identity theft, and misuse posed by his Private Information being placed in the hands of criminals.

103. Plaintiff Moraes has a continuing interest in ensuring that his Private Information, which remains in the possession of Defendant, is protected and safeguarded from future data

incidents. This interest is particularly acute, as Defendant's systems have already been shown to be susceptible to compromise and are subject to further compromise so long as Wellfleet fails to undertake the necessary and appropriate security and training measures to protect the Private Information in its possession.

104. As a result of the Data Incident, Plaintiff Moraes made reasonable efforts to mitigate the impact of the Data Incident, including but not limited to researching the Data Incident, reviewing accounts for any indications of actual or attempted identity theft or fraud, and researching the credit monitoring offered by Defendant. Plaintiff Moraes has spent several hours dealing with the Data Incident, which is valuable time he otherwise would have spent on other activities.

105. As a result of the Data Incident, Plaintiff Moraes has suffered anxiety as a result of the release of his Private Information, which he believed would be protected from unauthorized access and disclosure. These feelings include anxiety about unauthorized parties viewing, selling, and/or using his Private Information for purposes of committing cyber and other crimes against his including, but not limited to, fraud and identity theft. Plaintiff Moraes is very concerned about this increased, substantial, and continuing risk, as well as the consequences that identity theft and fraud resulting from the Data Incident would have on his life.

106. Plaintiff Moraes also suffered actual injury from having his Private Information compromised as a result of the Data Incident in the form of (a) damage to and diminution in the value of his Private Information, a form of property that Defendant obtained from Plaintiff; (b) violation of his privacy rights; and (c) present, imminent, and impending injury arising from the increased risk of identity theft, and fraud he now faces.

107. As a result of the Data Incident, Plaintiff Moraes anticipates spending considerable time and money on an ongoing basis to try to mitigate and address the many harms caused by the Data Incident.

108. Plaintiff and Class Members also face a substantial risk of being targeted in future phishing, data intrusion, and other illegal schemes through the misuse of their Private Information, since potential fraudsters will likely use such Private Information to carry out such targeted schemes against Plaintiff and Class Members.

109. The Private Information maintained by and stolen from Defendant's systems, combined with publicly available information, allows nefarious actors to assemble a detailed mosaic of Plaintiff and Class Members, which can also be used to carry out targeted fraudulent schemes against Plaintiff and Class Members.

110. Plaintiff and Class Members also lost the benefit of the bargain they made with Wellfleet. Plaintiff and Class Members overpaid for services that were intended to be accompanied by adequate data security but were not. Indeed, part of the price Plaintiff and Class Members paid to Wellfleet was intended to be used by Wellfleet to fund adequate security of Wellfleet's system and protect Plaintiff's and Class Members' Private Information. Thus, Plaintiff and the Class did not receive the benefit of the bargain.

111. As a result of the Data Incident, Plaintiff's and Class Members' Private Information, which has an inherent market value in both legitimate and illegal markets, has been harmed and diminished due to its acquisition by cybercriminals. This transfer of valuable information happened with no consideration paid to Plaintiff or Class Members for their property, resulting in an economic loss. Moreover, the Private Information is apparently readily available to others, and the rarity of the Private Information has been destroyed because it is no

longer only held by Plaintiff and the Class Members, and because that data no longer necessarily correlates only with activities undertaken by Plaintiff and the Class Members, thereby causing additional loss of value.

112. Finally, Plaintiff and Class Members have suffered or will suffer actual injury as a direct and proximate result of the Data Incident in the form of out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Incident.

113. Moreover, Plaintiff and Class Members have an interest in ensuring that their Private Information, which is believed to still be in the possession of Wellfleet, is protected from future data security incidents by the implementation of more adequate data security measures and safeguards, including but not limited to, ensuring that the storage of data or documents containing highly sensitive personal and health information in its possession is not accessible online, that access to such data is password-protected, and that such data is properly encrypted.

114. As a direct and proximate result of Wellfleet's actions and inactions, Plaintiff and Class Members have suffered a loss of privacy and have suffered cognizable harm, including an imminent and substantial future risk of harm, in the forms set forth above.

V. CLASS ACTION ALLEGATIONS

115. Plaintiff brings this action individually and on behalf of all other persons similarly situated, pursuant to Federal Rule of Civil Procedure 23(a), 23(b)(1), 23(b)(2), and 23(b)(3).

116. Specifically, Plaintiff proposes the following Nationwide Class (referred to herein as the "Class"), subject to amendment as appropriate:

> **Nationwide Class**
>
> All individuals in the United States whose Private Information was impacted as a result of the Data Incident, including all who were sent a Notice of Data Security Incident.

117. Excluded from the Class are Defendant and its parents or subsidiaries, any entities in which it has a controlling interest, as well as its officers, directors, affiliates, legal representatives, heirs, predecessors, successors, and assigns. Also excluded is any Judge to whom this case is assigned as well as their judicial staff and immediate family members.

118. Plaintiff reserves the right to modify or amend the definitions of the proposed Nationwide Class, as well as the addition of any subclasses, before the Court determines whether certification is appropriate.

119. The proposed Class meets the criteria for certification under Fed. R. Civ. P. 23(a), (b)(2), and (b)(3).

120. Numerosity. The Class Members are so numerous that joinder of all members is impracticable. Though the exact number and identities of Class Members are unknown at this time, based on information and belief, the Class consists of tens of thousands of individuals whose data was impacted in the Data Incident. The identities of Class Members are ascertainable through Wellfleet's records, Class Members' records, publication notice, self-identification, and other means.

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

a. Whether Wellfleet engaged in the conduct alleged herein;

b. Whether Wellfleet's conduct violated the FTCA, HIPAA, and/or Mass. 201 CMR 17.00;

c. When Wellfleet learned of the Data Incident;

d. Whether Wellfleet's response to the Data Incident was adequate;

e. Whether Wellfleet unlawfully lost or disclosed Plaintiff's and Class Members' Private Information;

f. Whether Wellfleet failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the Private Information compromised in the Data Incident;

g. Whether Wellfleet's data security systems prior to and during the Data Incident complied with applicable data security laws and regulations;

h. Whether Wellfleet's data security systems prior to and during the Data Incident were consistent with industry standards;

i. Whether Wellfleet owed a duty to Class Members to safeguard their Private Information;

j. Whether Wellfleet breached its duty to Class Members to safeguard their Private Information;

k. Whether cybercriminals obtained Class Members' Private Information via the Data Incident;

l. Whether Wellfleet had a legal duty to provide timely and accurate notice of the Data Incident to Plaintiff and the Class Members;

m. Whether Wellfleet breached its duty to provide timely and accurate notice of the Data Incident to Plaintiff and Class Members;

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

o. What damages Plaintiff and Class Members suffered as a result of Wellfleet's misconduct;

p. Whether Wellfleet's conduct was negligent;

q. Whether Wellfleet's conduct was *per se* negligent;

r. Whether Wellfleet was unjustly enriched;

s. Whether Plaintiff and Class Members are entitled to actual and/or statutory damages;

t. Whether Plaintiff and Class Members are entitled to additional credit or identity monitoring and monetary relief; and

u. Whether Plaintiff and Class Members are entitled to equitable relief, including injunctive relief, restitution, disgorgement, and/or the establishment of a constructive trust.

122. Typicality. Plaintiff's claims are typical of those of other Class Members because Plaintiff's Private Information, like that of every other Class Member, was compromised in the Data Incident. Plaintiff's claims are typical of those of the other Class Members because, *inter alia*, all Class Members were injured through the common misconduct of Wellfleet. Plaintiff is advancing the same claims and legal theories on behalf of himself and all other Class Members, and there are no defenses that are unique to Plaintiff. The claims of Plaintiff and those of Class Members arise from the same operative facts and are based on the same legal theories.

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

124. Predominance. Wellfleet has engaged in a common course of conduct toward Plaintiff and Class Members in that all of Plaintiff's and Class Members' data was stored on the same computer systems and unlawfully disclosed to the public in the same way. The common

issues arising from Wellfleet'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.

125. Superiority. A Class action is superior to other available methods for the fair and efficient adjudication of this controversy and no unusual difficulties are likely to be encountered in the management of this class action. 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 Wellfleet. In contrast, conducting this action as a class action presents far fewer management difficulties, conserves judicial resources and the parties' resources, and protects the rights of each Class Member.

126. Class certification is also appropriate under Fed. R. Civ. P. 23(b)(2). Wellfleet has acted and/or refused to act on grounds generally applicable to the Class such that final injunctive relief and/or corresponding declaratory relief is appropriate as to the Class as a whole.

127. Finally, all members of the proposed Class are readily ascertainable. Wellfleet has access to the names and addresses and/or email addresses of Class Members affected by the Data Incident. Class Members have already been preliminarily identified and sent notice of the Data Incident by Wellfleet.

CLAIMS FOR RELIEF

COUNT I
NEGLIGENCE
(ON BEHALF OF PLAINTIFF AND THE NATIONWIDE CLASS)

128. Plaintiff restates and realleges all of the allegations stated above as if fully set forth herein.

129. Wellfleet knowingly collected, came into possession of, and maintained Plaintiff's and Class Members' Private Information, and had a duty to exercise reasonable care in safeguarding, securing, and protecting such Information from being disclosed, compromised, lost, stolen, and/or misused by unauthorized parties.

130. Wellfleet knew or should have known of the risks inherent in collecting the Private Information of Plaintiff and Class Members and the importance of adequate security. Wellfleet was on notice because, on information and belief, it knew or should have known the value of such Private Information to cybercriminals.

131. Wellfleet owed a duty of care to Plaintiff and Class Members whose Private Information was entrusted to it. Wellfleet's duties included, but were not limited to, the following:

a. To exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting Private Information in its possession;

b. To protect the Private Information in its possession using reasonable and adequate security procedures and systems compliant with industry standards;

c. To have procedures in place to prevent the loss or unauthorized dissemination of Private Information in its possession;

d. To employ reasonable security measures and otherwise protect the Private Information of Plaintiff and Class Members pursuant to HIPAA, the FTCA and Mass. 201 CMR 17.00;

e. To implement processes to quickly detect a data incident like this; and

f. To promptly notify Plaintiff and Class Members of the Data Incident, and to precisely disclose the type(s) of information compromised.

132. Wellfleet's duty to employ reasonable data security measures arose, in part, under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data.

133. Wellfleet's duty also arose because Defendant was bound by industry standards to protect the confidential Private Information, which includes PHI, in its possession.

134. Plaintiff and Class Members were foreseeable victims of any inadequate security practices on the part of Defendant, and Wellfleet owed them a duty of care to not subject them to an unreasonable risk of harm.

135. Wellfleet, through its actions and/or omissions, unlawfully breached its duty to Plaintiff and Class Members by failing to exercise reasonable care in protecting and safeguarding Plaintiff's and Class Members' Private Information within its possession.

136. Wellfleet, by its actions and/or omissions, breached its duty of care by failing to provide, or acting with reckless disregard for, fair, reasonable, or adequate computer systems and data security practices to safeguard the Private Information of Plaintiff and Class Members.

137. Wellfleet, by its actions and/or omissions, breached its duty of care by failing to promptly identify the Data Incident and then failing to provide prompt notice of the Data Incident to the persons whose Private Information was compromised.

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

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

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

c. Failing to periodically ensure that its email system maintained reasonable data security safeguards;

d. Allowing unauthorized access to Class Members' Private Information; and

e. Failing to comply with the FTCA, HIPPA, and Mass. 201 CMR 17.00.

139. Wellfleet had a special relationship with Plaintiff and Class Members. Plaintiff's and Class Members' willingness to entrust Wellfleet with their Private Information was predicated on the understanding that Wellfleet would take adequate security precautions. Moreover, only Wellfleet had the ability to protect its systems (and the Private Information that it stored on them) from unauthorized disclosure.

140. Wellfleet's breach of duties owed to Plaintiff and Class Members caused Plaintiff's and Class Members' Private Information to be compromised, as alleged herein.

141. Wellfleet's breaches of duty also caused a substantial, imminent risk to Plaintiff and Class Members of identity theft, loss of control over their Private Information, and/or loss of time and money to monitor their accounts for fraud.

142. As a result of Wellfleet's negligence in breach of its duties owed to Plaintiff and Class Members, Plaintiff and Class Members are in danger of imminent harm in that their Private Information, which is still likely in the possession of unauthorized third parties, will be used for fraudulent purposes.

143. Wellfleet also had independent duties under state laws that required it to reasonably safeguard Plaintiff's and Class Members' Private Information and promptly notify them about the Data Incident.

144. As a direct and proximate result of Wellfleet's negligent conduct, Plaintiff and Class Members have suffered damages as alleged herein and are at imminent risk of further harm.

145. The injury and harm that Plaintiff and Class Members suffered was reasonably foreseeable.

146. Plaintiff and Class Members have suffered injury and are entitled to damages in an amount to be proven at trial.

147. In addition to monetary relief, Plaintiff and Class Members are also entitled to injunctive relief requiring Wellfleet to, *inter alia*, strengthen its data security systems and monitoring procedures, conduct periodic audits of those systems, and provide lifetime credit monitoring and identity theft insurance to Plaintiff and Class Members.

COUNT II
NEGLIGENCE *PER SE*
(ON BEHALF OF PLAINTIFF AND THE NATIONWIDE CLASS)

148. Plaintiff restates and realleges the allegations in the preceding paragraphs as if fully set forth herein.

149. Pursuant to Section 5 of the FTCA, Wellfleet had a duty to provide fair and adequate computer systems and data security to safeguard the Private Information of Plaintiff and Class Members.

150. Further, Mass. 201 CMR 17.00 requires companies, like Defendant, to meet minimum standards in connection with the safeguarding of personal information contained in both paper and electronic records to insure the security and confidentiality of customer information in a manner fully consistent with industry standards; protect against anticipated threats or hazards to the security or integrity of such information; and protect against unauthorized access to or use of such information that may result in substantial harm or inconvenience to any consumer.

151. Additionally, pursuant to HIPAA, 42 U.S.C. § 1302(d), *et seq*., Wellfleet had a duty to implement reasonable safeguards to protect Plaintiff's and Class Members' Private Information. Specifically, pursuant to HIPAA, Defendant had a duty to render the electronic PHI it maintained unusable, unreadable, or indecipherable to unauthorized individuals by "the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without the use of a confidential process or key." *See* definition of "encryption" at 45 C.F.R. § 164.304.

152. Wellfleet breached its duties to Plaintiff and Class Members under the FTCA, HIPAA, and Mass. 201 CMR 17.00 by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiff's and Class Members' Private Information.

153. Specifically, Wellfleet breached its duties by failing to employ industry-standard cybersecurity measures in order to comply with the FTCA.

154. The FTCA prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice of failing to use reasonable measures to protect PII and PHI (such as the Private Information compromised in the Data Incident). The FTC rulings and publications described above, together with the industry-standard cybersecurity measures set forth herein, form part of the basis of Wellfleet's duty in this regard.

155. Wellfleet also violated the FTCA, HIPAA, and Mass. 201 CMR 17.00 by failing to use reasonable measures to protect the Private Information of Plaintiff and the Class and by not complying with applicable industry standards, as described herein.

156. It was reasonably foreseeable that the failure to reasonably protect and secure Plaintiff's and Class Members' Private Information in compliance with applicable laws would result in an unauthorized third-party gaining access to Wellfleet's networks, databases, and computers that stored Plaintiff's and Class Members' unencrypted Private Information.

157. Plaintiff and Class Members are within the class of persons that the FTCA, HIPAA, and Mass. 201 CMR 17.00 are intended to protect and Wellfleet's failure to comply with both constitutes negligence *per se*.

158. Plaintiff's and Class Members' Private Information constitutes personal property that was compromised due to Wellfleet's negligence, resulting in harm, injury, and damages to Plaintiff and Class Members.

159. As a direct and proximate result of Wellfleet's negligence *per se*, Plaintiff and the Class have suffered, and continue to suffer, injuries and damages arising from the unauthorized sharing of their Private Information, including but not limited to, damages from the lost time and effort to mitigate the actual and potential impact of the Data Incident on their lives.

160. As a direct and proximate result of Wellfleet's negligent conduct, Plaintiff and Class Members have suffered injury and are entitled to compensatory and consequential damages in an amount to be proven at trial.

161. In addition to monetary relief, Plaintiff and Class Members are also entitled to injunctive relief requiring Wellfleet to, *inter alia*, strengthen its data security systems, website, and monitoring procedures, conduct periodic audits of those systems and website, and provide lifetime credit monitoring and identity theft insurance to Plaintiff and Class Members.

COUNT III
BREACH OF IMPLIED CONTRACT
(ON BEHALF OF PLAINTIFF AND THE NATIONWIDE CLASS)

162. Plaintiff restates and realleges the allegations in the preceding paragraphs as if fully set forth herein.

163. Wellfleet provides health insurance and other services to Plaintiff and Class Members. Plaintiff and Class Members formed an implied contract with Defendant regarding the provision of those services through their collective conduct, including by Plaintiff and Class Members paying for services and/or entrusting their valuable Private Information to Defendant in exchange for such services.

164. Through Defendant's provision of insurance services to Plaintiff and Class Members, it knew or should have known that it must protect Plaintiff's and Class Members' confidential Private Information in accordance with its policies, practices, and applicable law.

165. As consideration, Plaintiff and Class Members paid money to Wellfleet and/or turned over valuable Private Information to Wellfleet. Accordingly, Plaintiff and Class Members bargained with Wellfleet to securely maintain and store their Private Information.

166. Wellfleet accepted payment and/or possession of Plaintiff's and Class Members' Private Information for the purpose of providing services to Plaintiff and Class Members.

167. In paying Defendant and/or providing their valuable Private Information to Defendant in exchange for Defendant's services, Plaintiff and Class Members intended and understood that Wellfleet would adequately safeguard the Private Information as part of those services.

168. Defendant's implied promises to Plaintiff and Class Members include, but are not limited to, (1) taking steps to ensure that anyone who is granted access to Private Information also protect the confidentiality of that data; (2) taking steps to ensure that the Private Information that is placed in the control of its employees is restricted and limited to achieve an authorized business purpose; (3) restricting access to the Private Information to qualified and trained employees and/or agents; (4) designing and implementing appropriate retention policies to protect the Private Information against unauthorized disclosure; (5) applying or requiring proper encryption; (6) implementing multifactor authentication for access; and (7) complying with HIPAA standards to make sure that Plaintiff's and Class Members' PHI would remain protected.

169. Plaintiff and Class Members would not have entrusted their Private Information to Wellfleet in the absence of such an implied contract.

170. Had Wellfleet disclosed to Plaintiff and the Class that it did not have adequate an adequate website, computer systems, and/or security practices to secure sensitive data, Plaintiff and Class Members would not have provided their Private Information to Wellfleet.

171. As a provider of healthcare insurance, Wellfleet recognized (or should have recognized) that Plaintiff's and Class Member's Private Information is highly sensitive and must

be protected, and that this protection was of material importance as part of its bargain with Plaintiff and the other Class Members.

172. Wellfleet violated these implied contracts by failing to employ reasonable and adequate security measures to secure Plaintiff's and Class Members' Private Information. Wellfleet further breached these implied contracts by failing to abide by HIPAA.

173. Additionally, Wellfleet breached the implied contracts with Plaintiff and Class Members by failing to ensure the confidentiality and integrity of electronic protected health information it created, received, maintained, and transmitted, in violation of 45 CFR 164.306(a)(1).

174. Wellfleet also breached the implied contracts with Plaintiff and Class Members by failing to implement technical policies and procedures for electronic 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 CFR 164.312(a)(1).

175. Wellfleet further breached the implied contracts with Plaintiff and Class Members by failing to implement policies and procedures to prevent, detect, contain, and correct security violations, in violation of 45 CFR 164.308(a)(1).

176. Wellfleet further breached the implied contracts with Plaintiff and Class Members by failing to identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity, in violation of 45 CFR 164.308(a)(6)(ii).

177. Wellfleet further breached the implied contracts with Plaintiff and Class Members by failing to protect against any reasonably anticipated threats or hazards to the security or integrity of electronic protected health information, in violation of 45 CFR 164.306(a)(2).

178. Wellfleet further breached the implied contracts with Plaintiff and Class Members by failing to protect against any reasonably anticipated uses or disclosures of electronic protected health information that are not permitted under the privacy rules regarding individually identifiable health information, in violation of 45 CFR 164.306(a)(3).

179. Wellfleet further breached the implied contracts with Plaintiff and Class Members by failing to ensure compliance with the HIPAA security standard rules by its workforce violations, in violation of 45 CFR 164.306(a)(94).

180. Wellfleet further breached the implied contracts with Plaintiff and Class Members by impermissibly and improperly using and disclosing protected health information that is and remains accessible to unauthorized persons, in violation of 45 CFR 164.502, *et seq*.

181. Wellfleet further breached the implied contracts with Plaintiff and Class Members by failing to design, implement, and enforce policies and procedures establishing physical administrative safeguards to reasonably safeguard protected health information, in violation of 45 CFR 164.530(c).

182. Wellfleet further breached the implied contracts with Plaintiff and Class Members by otherwise failing to safeguard Plaintiff's and Class Members' PHI.

183. A meeting of the minds occurred, as Plaintiff and Class Members agreed, *inter alia*, to provide payment and/or accurate and complete Private Information to Wellfleet in exchange for Wellfleet's agreement to, *inter alia*, provide services that included protection of their highly sensitive Private Information.

184. Plaintiff and Class Members have been damaged by Wellfleet's conduct, including the harms and injuries arising from the Data Incident now and in the future, as alleged herein.

COUNT IV
UNJUST ENRICHMENT
(ON BEHALF OF PLAINTIFF AND THE NATIONWIDE CLASS)

185. Plaintiff restates and realleges the allegations in the preceding paragraphs as if fully set forth herein.

186. This Count is pleaded in the alternative to Count III above.

187. Plaintiff and Class Members conferred a benefit on Wellfleet by paying for insurance services that should have included cybersecurity protection to protect their Private Information and/or turning over their Private Information to Defendant in exchange for the security of such Private Information. Plaintiff and Class Members did not receive such protection.

188. Wellfleet knew that Plaintiff and Class Members conferred a benefit upon it, which Wellfleet accepted. Wellfleet profited from these transactions and used the Private Information of Plaintiff and Class Members for business purposes, while failing to use these benefits for adequate data security measures that would have secured Plaintiff's and Class Members' Private Information and prevented the Data Incident.

189. If Plaintiff and Class Members had known that Wellfleet had not adequately secured their Private Information, they would not have agreed to provide such Private Information to Defendant.

190. Due to Wellfleet's conduct alleged herein, it would be unjust and inequitable under the circumstances for Wellfleet to be permitted to retain the benefit of its wrongful conduct.

191. As a direct and proximate result of Wellfleet's conduct, Plaintiff and Class Members have suffered, and/or are at a continued, imminent risk of suffering, injury that

includes but is not limited to the following: (i) the loss of the opportunity to control how their Private Information is used; (ii) the compromise, publication, and/or theft of their Private Information; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, and/or unauthorized use of their Private Information; (iv) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Incident, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (v) the continued risk to their Private Information, which remains in Wellfleet's possession and is subject to further unauthorized disclosures so long as Wellfleet fails to undertake appropriate and adequate measures to protect Private Information in its continued possession; and (vi) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the Private Information compromised as a result of the Data Incident for the remainder of the lives of Plaintiff and Class Members.

192. Plaintiff and Class Members are entitled to full refunds, restitution, and/or damages from Wellfleet and/or an order proportionally disgorging all profits, benefits, and other compensation obtained by Wellfleet from its wrongful conduct. This can be accomplished by establishing a constructive trust from which the Plaintiff and Class Members may seek restitution or compensation.

193. Plaintiff and Class Members may not have an adequate remedy at law against Wellfleet, and accordingly, they plead this claim for unjust enrichment in addition to, or in the alternative to, other claims pleaded herein.

COUNT V
DECLARATORY JUDGMENT
(ON BEHALF OF PLAINTIFF AND THE NATIONWIDE CLASS)

194. Plaintiff restates and realleges the allegations in the preceding paragraphs as if fully set forth herein.

195. Under the Declaratory Judgment Act, 28 U.S.C. § 2201, *et seq.*, this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and to grant further necessary relief. Furthermore, the Court has broad authority to restrain acts that are tortious and violate the terms of the federal laws and regulations described in this Complaint.

196. Wellfleet owes a duty of care to Plaintiff and Class Members, which required it to adequately secure Plaintiff's and Class Members' Private Information.

197. Wellfleet still possesses Private Information regarding Plaintiff and Class Members.

198. Plaintiff alleges that Wellfleet's data security measures remain inadequate. Furthermore, Plaintiff continue to suffer injury as a result of the illegal and unauthorized sharing of their Private Information and the risk remains that further compromise of their Private Information will occur in the future.

199. Under its authority pursuant to the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following:

a. Wellfleet owes a legal duty to secure the Private Information in its possession and to timely notify individuals of the unauthorized disclosure of their Private Information under the common law, HIPAA, Mass. 201 CMR 17.00, and the FTCA;

b. Wellfleet's existing security measures do not comply with its explicit or implicit contractual obligations and duties of care to provide reasonable security procedures and practices that are appropriate to protect the Private Information in its possession; and

c. Wellfleet continues to breach this legal duty by failing to employ reasonable measures to secure the Private Information in its possession.

200. This Court should also issue corresponding prospective injunctive relief requiring Wellfleet to employ adequate security protocols consistent with legal and industry standards to protect customers' Private Information, including the following:

a. Order Wellfleet to provide lifetime credit monitoring and identity theft insurance to Plaintiff and Class Members.

b. Order that, to comply with Defendant's explicit or implicit contractual obligations and duties of care, Wellfleet must implement and maintain reasonable security measures, including, but not limited to:

i. engaging third-party security auditors to conduct testing, including simulated attacks, penetration tests, and audits on Wellfleet's systems and website on a periodic basis, and ordering Wellfleet to promptly correct any problems or issues detected by such third-party security auditors;

ii. engaging third-party security auditors and internal personnel to run automated security monitoring;

iii. auditing, testing, and training its security personnel regarding any new or modified procedures;

iv. segmenting its user applications by, among other things, creating firewalls and access controls so that if one area is compromised, unauthorized access to other portions of Wellfleet's systems cannot be achieved;

v. conducting regular database scanning and security checks; and

vi. routinely and continually conducting internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach.

201. If an injunction is not issued, Plaintiff will suffer irreparable injury and will lack an adequate legal remedy to prevent another similar incident at Wellfleet. The risk of another such incident is real, immediate, and substantial. If another incident like this occurs at Wellfleet, Plaintiff will not have an adequate remedy at law because many of the resulting injuries are not readily quantifiable.

202. The hardship to Plaintiff if an injunction is not issued exceeds the hardship to Wellfleet if an injunction is issued. Plaintiff will likely be subjected to substantial, continued identity theft and other related damages if an injunction is not issued. On the other hand, the cost of Wellfleet's compliance with an injunction requiring reasonable prospective data security measures is relatively minimal, and Wellfleet has a pre-existing legal obligation to employ such measures.

203. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing a subsequent data incident at Wellfleet, thus preventing future injury to Plaintiff and other individuals whose Private Information would be further compromised.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of himself and the Class described above, seek the following relief:

a. An order certifying this action as a Class action under Fed. R. Civ. P. 23, defining the Class as requested herein, appointing the undersigned as Class counsel, and finding that Plaintiff is a proper representative of the Nationwide Class requested herein;

b. Judgment in favor of Plaintiff and Class Members awarding them appropriate monetary relief, including actual damages, statutory damages, equitable relief, restitution, disgorgement, and statutory costs;

c. An order providing injunctive and other equitable relief as necessary to protect the interests of the Class as requested herein;

d. An order instructing Wellfleet to purchase or provide funds for lifetime credit monitoring and identity theft insurance to Plaintiff and Class Members;

e. An order requiring Wellfleet to pay the costs involved in notifying Class Members about the judgment and administering the claims process;

f. A judgment in favor of Plaintiff and Class Members awarding them prejudgment and post-judgment interest, reasonable attorneys' fees, costs, and expenses as allowable by law; and

g. An award of such other and further relief as this Court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiff demands a trial by jury on all triable issues.

DATED: October 25, 2024

Respectfully submitted,

/s/ Christina Xenides

Christina Xenides, Esq.
Massachusetts Bar No. 677603
SIRI & GLIMSTAD LLP
1005 Congress Avenue, Suite 925-C36
Austin, TX 78701
Telephone: (512) 265-5622
E: cxenides@sirillp.com

Tyler J. Bean, Esq.
SIRI & GLIMSTAD LLP
745 Fifth Avenue, Suite 500
New York, New York 10151
Tel: (212) 532-1091
E: tbean@sirillp.com

Counsel for Plaintiff Moraes and the Putative Class

JS 44 (Rev. 10/20)

CIVIL COVER SHEET

The JS 44 civil cover sheet and the information contained herein neither replace nor supplement the filing and service of pleadings or other papers as required by law, except as provided by local rules of court. This form, approved by the Judicial Conference of the United States in September 1974, is required for the use of the Clerk of Court for the purpose of initiating the civil docket sheet. *(SEE INSTRUCTIONS ON NEXT PAGE OF THIS FORM.)*

I. (a) PLAINTIFFS

Jose Moraes

(b) County of Residence of First Listed Plaintiff Oklahoma, Oklahoma
(EXCEPT IN U.S. PLAINTIFF CASES)

(c) Attorneys *(Firm Name, Address, and Telephone Number)*

Christina Xenides, Esq.
Siri & Glimstad LLP, 1005 Congress Avenue, Suite 925-C36, Austin, TX 78701
Telephone: 512-265-5622

DEFENDANTS

Wellfleet Group, LLC

County of Residence of First Listed Defendant Hampden, Massachusetts
(IN U.S. PLAINTIFF CASES ONLY)

NOTE: IN LAND CONDEMNATION CASES, USE THE LOCATION OF THE TRACT OF LAND INVOLVED.

Attorneys *(If Known)*

II. BASIS OF JURISDICTION *(Place an "X" in One Box Only)*

- ☐ 1 U.S. Government Plaintiff
- ☐ 3 Federal Question *(U.S. Government Not a Party)*
- ☐ 2 U.S. Government Defendant
- ☒ 4 Diversity *(Indicate Citizenship of Parties in Item III)*

III. CITIZENSHIP OF PRINCIPAL PARTIES *(Place an "X" in One Box for Plaintiff and One Box for Defendant)*

(For Diversity Cases Only)

	PTF	DEF		PTF	DEF
Citizen of This State	☐ 1	☐ 1	Incorporated *or* Principal Place of Business In This State	☐ 4	☒ 4
Citizen of Another State	☒ 2	☐ 2	Incorporated *and* Principal Place of Business In Another State	☐ 5	☐ 5
Citizen or Subject of a Foreign Country	☐ 3	☐ 3	Foreign Nation	☐ 6	☐ 6

IV. NATURE OF SUIT *(Place an "X" in One Box Only)*

Click here for: Nature of Suit Code Descriptions.

CONTRACT
- ☐ 110 Insurance
- ☐ 120 Marine
- ☐ 130 Miller Act
- ☐ 140 Negotiable Instrument
- ☐ 150 Recovery of Overpayment & Enforcement of Judgment
- ☐ 151 Medicare Act
- ☐ 152 Recovery of Defaulted Student Loans (Excludes Veterans)
- ☐ 153 Recovery of Overpayment of Veteran's Benefits
- ☐ 160 Stockholders' Suits
- ☐ 190 Other Contract
- ☐ 195 Contract Product Liability
- ☐ 196 Franchise

REAL PROPERTY
- ☐ 210 Land Condemnation
- ☐ 220 Foreclosure
- ☐ 230 Rent Lease & Ejectment
- ☐ 240 Torts to Land
- ☐ 245 Tort Product Liability
- ☐ 290 All Other Real Property

TORTS

PERSONAL INJURY
- ☐ 310 Airplane
- ☐ 315 Airplane Product Liability
- ☐ 320 Assault, Libel & Slander
- ☐ 330 Federal Employers' Liability
- ☐ 340 Marine
- ☐ 345 Marine Product Liability
- ☐ 350 Motor Vehicle
- ☐ 355 Motor Vehicle Product Liability
- ☐ 360 Other Personal Injury
- ☐ 362 Personal Injury - Medical Malpractice

PERSONAL INJURY
- ☐ 365 Personal Injury - Product Liability
- ☐ 367 Health Care/ Pharmaceutical Personal Injury Product Liability
- ☐ 368 Asbestos Personal Injury Product Liability

PERSONAL PROPERTY
- ☐ 370 Other Fraud
- ☐ 371 Truth in Lending
- ☒ 380 Other Personal Property Damage
- ☐ 385 Property Damage Product Liability

CIVIL RIGHTS
- ☐ 440 Other Civil Rights
- ☐ 441 Voting
- ☐ 442 Employment
- ☐ 443 Housing/ Accommodations
- ☐ 445 Amer. w/Disabilities - Employment
- ☐ 446 Amer. w/Disabilities - Other
- ☐ 448 Education

PRISONER PETITIONS

Habeas Corpus:
- ☐ 463 Alien Detainee
- ☐ 510 Motions to Vacate Sentence
- ☐ 530 General
- ☐ 535 Death Penalty

Other:
- ☐ 540 Mandamus & Other
- ☐ 550 Civil Rights
- ☐ 555 Prison Condition
- ☐ 560 Civil Detainee - Conditions of Confinement

FORFEITURE/PENALTY
- ☐ 625 Drug Related Seizure of Property 21 USC 881
- ☐ 690 Other

LABOR
- ☐ 710 Fair Labor Standards Act
- ☐ 720 Labor/Management Relations
- ☐ 740 Railway Labor Act
- ☐ 751 Family and Medical Leave Act
- ☐ 790 Other Labor Litigation
- ☐ 791 Employee Retirement Income Security Act

IMMIGRATION
- ☐ 462 Naturalization Application
- ☐ 465 Other Immigration Actions

BANKRUPTCY
- ☐ 422 Appeal 28 USC 158
- ☐ 423 Withdrawal 28 USC 157

PROPERTY RIGHTS
- ☐ 820 Copyrights
- ☐ 830 Patent
- ☐ 835 Patent - Abbreviated New Drug Application
- ☐ 840 Trademark
- ☐ 880 Defend Trade Secrets Act of 2016

SOCIAL SECURITY
- ☐ 861 HIA (1395ff)
- ☐ 862 Black Lung (923)
- ☐ 863 DIWC/DIWW (405(g))
- ☐ 864 SSID Title XVI
- ☐ 865 RSI (405(g))

FEDERAL TAX SUITS
- ☐ 870 Taxes (U.S. Plaintiff or Defendant)
- ☐ 871 IRS—Third Party 26 USC 7609

OTHER STATUTES
- ☐ 375 False Claims Act
- ☐ 376 Qui Tam (31 USC 3729(a))
- ☐ 400 State Reapportionment
- ☐ 410 Antitrust
- ☐ 430 Banks and Banking
- ☐ 450 Commerce
- ☐ 460 Deportation
- ☐ 470 Racketeer Influenced and Corrupt Organizations
- ☐ 480 Consumer Credit (15 USC 1681 or 1692)
- ☐ 485 Telephone Consumer Protection Act
- ☐ 490 Cable/Sat TV
- ☐ 850 Securities/Commodities/ Exchange
- ☐ 890 Other Statutory Actions
- ☐ 891 Agricultural Acts
- ☐ 893 Environmental Matters
- ☐ 895 Freedom of Information Act
- ☐ 896 Arbitration
- ☐ 899 Administrative Procedure Act/Review or Appeal of Agency Decision
- ☐ 950 Constitutionality of State Statutes

V. ORIGIN *(Place an "X" in One Box Only)*

☒ 1 Original Proceeding | ☐ 2 Removed from State Court | ☐ 3 Remanded from Appellate Court | ☐ 4 Reinstated or Reopened | ☐ 5 Transferred from Another District *(specify)* | ☐ 6 Multidistrict Litigation - Transfer | ☐ 8 Multidistrict Litigation - Direct File

VI. CAUSE OF ACTION

Cite the U.S. Civil Statute under which you are filing ***(Do not cite jurisdictional statutes unless diversity)***:
28 U.S.C. § 1332(d)

Brief description of cause:
Plaintiff brings this action against Defendant for their failure to properly secure and safeguard Plaintiff's personal and sensitive information.

VII. REQUESTED IN COMPLAINT:

☒ CHECK IF THIS IS A **CLASS ACTION** UNDER RULE 23, F.R.Cv.P.

DEMAND $ $5,000,000

CHECK YES only if demanded in complaint:
JURY DEMAND: ☒ Yes ☐ No

VIII. RELATED CASE(S) IF ANY

(See instructions): JUDGE _____ DOCKET NUMBER _____

DATE 10/25/2024

SIGNATURE OF ATTORNEY OF RECORD */s/ Christina Xenides*

FOR OFFICE USE ONLY

RECEIPT # _____ AMOUNT _____ APPLYING IFP _____ JUDGE _____ MAG. JUDGE _____

UNITED STATES DISTRICT COURT
DISTRICT OF MASSACHUSETTS

1. **Title of case (name of first party on each side only)** Jose Moraes v. Wellfleet Group, LLC

2. **Category in which the case belongs based upon the numbered nature of suit code listed on the civil cover sheet. (See local rule 40.1(a)(1)).**

☐ **I.** **160, 400, 410, 441, 535, 830*, 835*, 850, 880, 891, 893, R.23, REGARDLESS OF NATURE OF SUIT.**

☐ **II.** **110, 130, 190, 196, 370, 375, 376, 440, 442, 443, 445, 446, 448, 470, 751, 820*, 840*, 895, 896, 899.**

☑ **III.** **120, 140, 150, 151, 152, 153, 195, 210, 220, 230, 240, 245, 290, 310, 315, 320, 330, 340, 345, 350, 355, 360, 362, 365, 367, 368, 371, 380, 385, 422, 423, 430, 450, 460, 462, 463, 465, 480, 485, 490, 510, 530, 540, 550, 555, 560, 625, 690, 710, 720, 740, 790, 791, 861-865, 870, 871, 890, 950.**
***Also complete AO 120 or AO 121. for patent, trademark or copyright cases.**

3. **Title and number, if any, of related cases. (See local rule 40.1(g)). If more than one prior related case has been filed in this district please indicate the title and number of the first filed case in this court.**

4. **Has a prior action between the same parties and based on the same claim ever been filed in this court?**
YES ☐ **NO** ☑

5. **Does the complaint in this case question the constitutionality of an act of congress affecting the public interest? (See 28 USC §2403)**
YES ☐ **NO** ☑
If so, is the U.S.A. or an officer, agent or employee of the U.S. a party?
YES ☐ **NO** ☐

6. **Is this case required to be heard and determined by a district court of three judges pursuant to title 28 USC §2284?**
YES ☐ **NO** ☑

7. **Do all of the parties in this action, excluding governmental agencies of the United States and the Commonwealth of Massachusetts ("governmental agencies"), residing in Massachusetts reside in the same division? - (See Local Rule 40.1(d)).**
YES ☑ **NO** ☐

A. **If yes, in which division do all of the non-governmental parties reside?**
Eastern Division ☐ **Central Division** ☐ **Western Division** ☑

B. **If no, in which division do the majority of the plaintiffs or the only parties, excluding governmental agencies, residing in Massachusetts reside?**
Eastern Division ☐ **Central Division** ☐ **Western Division** ☐

8. **If filing a Notice of Removal - are there any motions pending in the state court requiring the attention of this Court? (If yes, submit a separate sheet identifying the motions)**
YES ☐ **NO** ☐

(PLEASE TYPE OR PRINT)

ATTORNEY'S NAME Christina Xenides
ADDRESS Siri & Glimstad LLP, 1005 Congress Avenue, Suite 925-C36, Austin, TX 78701
TELEPHONE NO. (512) 265-5622