UNITED STATES DISTRICT COURT
DISTRICT OF MASSACHUSETTS

JASMYN BICKHAM AND AMANDA BAILEY, individually and on behalf of all others similarly situated, Plaintiff, v. REPROSOURCE FERTILITY DIAGNOSTICS, INC., Defendant.	Case No.: 1:21-cv-11879-GAO

FIRST AMENDED CLASS ACTION COMPLAINT

Plaintiffs Jasmyn Bickham ("Bickham" or "Plaintiff Bickham") and Amanda Bailey ("Bailey" or "Plaintiff Bailey") (collectively, "Plaintiffs"), individually and on behalf of all others similarly situated, through undersigned counsel, hereby allege the following against Defendant ReproSource Fertility Diagnostics, Inc. ("ReproSource" or "Defendant"). Facts pertaining to Plaintiffs and their personal experiences and circumstances are alleged on personal knowledge, and all other facts herein are alleged on information and belief, based on, *inter alia*, the investigation of Plaintiffs' counsel.

NATURE OF THE ACTION

1. This is a class action for damages with respect to ReproSource, for its failure to exercise reasonable care in securing and safeguarding its patients' sensitive personal data—including names, addresses, email addresses, dates of birth, Social Security numbers, health insurance billing information, and treating physician information, collectively known as personally identifiable information ("PII" or "Private Information").

2. This class action is brought on behalf of patients whose sensitive PII was stolen by cybercriminals in a cyber-attack on ReproSource's systems on or around August 8, 2021 that resulted in the access and exfiltration of sensitive patient information(the "Data Breach").

3. The Data Breach affected at least 350,000 individual customers of ReproSource's services.

4. ReproSource reported to Plaintiffs and members of the putative "Class" (defined below) that information compromised in the Data Breach included their PII.

5. Plaintiffs and Class members were not notified of the data breach until October 21, 2021 at the earliest, more than two months after their information was first accessed.

6. As a result of the Data Breach, Plaintiffs and other Class members have and will continue to experience various types of misuse of their PII in the coming months and years, including but not limited to unauthorized credit card charges, unauthorized access to email accounts, identity theft, and other fraudulent use of their financial accounts and Private Information.

7. There has been no assurance offered by ReproSource that all personal data or copies of data have been recovered or destroyed.

8. Accordingly, Plaintiffs assert claims for negligence, breach of contract, breach of implied contract, breach of fiduciary duty, and declaratory and injunctive relief.

PARTIES

A. Plaintiff Jasmyn Bickham

9. Plaintiff Jasmyn Bickham is a resident of Rhode Island and brings this action in her individual capacity and on behalf of all others similarly situated. Bickham visited a Fertility Solutions clinic in Providence, Rhode Island in 2015 for a doctor's appointment. To receive

services at Fertility Solutions, Plaintiff was required to disclose her PII, which was then entered into ReproSource's database and maintained by Defendant without her knowledge. In maintaining her information, Defendant expressly and impliedly promised to safeguard Plaintiff Bickham's PII. Defendant, however, did not take proper care of Bickham's PII, leading to its exposure to, and exfiltration by, cybercriminals as a direct result of Defendant's inadequate security measures.

10. In October of 2021, Plaintiff Bickham received a notification letter from Defendant stating that her PII, which included "names, addresses, phone number, email addresses, date[s] of birth, billing and health information, health insurance or group plan identification names and numbers provided by you or your treating physician," was compromised by cybercriminals.

11. The letter also offered one year of credit monitoring through Kroll, which was and continues to be ineffective for Bickham and other Class members. The Kroll credit monitoring would have shared Bickham's information with third parties and could not guarantee complete privacy of her sensitive PII.

12. Because it is indisputable that the compromised PII has already been fraudulently misused as a result of the Data Breach, Plaintiff Bickham and the other Class members face a certainly impending and substantial risk of a slew of future harms as a result of Defendant's ineffective data security measures, as further set forth herein. Some of these harms will include fraudulent charges, medical procedures ordered in patients' names without their permission, and targeted advertising without patient consent.

13. Plaintiff Bickham greatly values her privacy, especially in receiving medical services (and fertility services in particular), and she would not have paid the amount that she did for fertility services if she had known that her information would be maintained using inadequate data security systems.

B. Plaintiff Amanda Bailey

14. Plaintiff Amanda Bailey is a resident of North Carolina and brings this action in her individual capacity and on behalf of all others similarly situated. Plaintiff Bailey visited Reach Fertility Clinic in Mooresville North Carolina between late 2017 and early 2018 for scheduled treatments. To receive services at Reach Fertility Clinic, Plaintiff Bailey was required to disclose her PII, which was then entered into ReproSource's database and maintained by Defendant without her knowledge. In maintaining her information, Defendant expressly and impliedly promised to safeguard Plaintiff's PII. Defendant, however, did not take proper care of Plaintiff Bailey's PII, leading to its exposure to, and exfiltration by, cybercriminals as a direct result of Defendant's inadequate security measures.

15. In December of 2021, Plaintiff Bailey received a notification letter from Defendant stating that her PII, which included her "name, address, phone number, email address, date of birth, billing and health information, such as CPT codes, diagnosis codes, test requisitions and results, health insurance or group plan identification names and numbers provided by you or your treating physician," was compromised by cybercriminals.

16. Because it is indisputable that the compromised PII has already been fraudulently misused as a result of the Data Breach, Plaintiff Bailey and the other Class members face a certainly impending and substantial risk of a slew of harms as a result of Defendant's ineffective data security measures. Some of these harms will include fraudulent charges, medical procedures ordered in patients' names without their permission, and targeted advertising without patient consent.

17. Some of these harms have already materialized in Plaintiff Bailey's case. Immediately after Ms. Bailey received the notice letter notifying her that her information was

accessed by unauthorized actors due to Defendant's inadequate data security practices, she used the code provided in the letter to register for identity monitoring services through Kroll. Within approximately two weeks, Plaintiff Bailey received alerts through two credit reporting agencies on another credit monitoring software that her information had been used to fraudulently apply for bank accounts and loans in her name.

18. First, on December 30, 2021, Plaintiff Bailey was alerted through a TransUnion credit report that an unauthorized party opened a bank account and attempted to apply for a loan in her name at an Apple Federal Credit Union branch in Northern Virginia. The loan request was denied, but the inquiry continues to appear on her credit report.

19. Additionally, on December 30, 2021, Plaintiff Bailey was alerted to a second fraudulent loan attempt in her name through an Equifax credit report at an Arlington Community Federal Credit Union branch in Northern Virginia. The unauthorized actor again successfully opened a bank account in Plaintiff Bailey's name using fake identifying documents. Among these documents were a fake driver's license in Plaintiff Bailey's name issued in September of 2021, a fake local utility bill in Plaintiff Bailey's name with a fake address, and a fake paystub from Ronald Reagan airport containing her identifying information.

20. Plaintiff Bailey has worked diligently to remedy these fraudulent uses of her identifying information. In addition to reporting the fraudulent loan requests to the major credit agencies and freezing her accounts, Plaintiff Bailey spent time speaking to each of the bank branches mentioned above, clarifying that she did not request the loans, and closing the accounts that were fraudulently opened in her name. Plaintiff Bailey has also filed police reports related to both incidents with her local sheriff's office. Although both fraudulently opened accounts are

closed, the loan inquiries remain on her credit report despite multiple disputes with her credit reporting agencies.

21. The fraudulent use of Plaintiff Bailey's information for loan inquiries made by unauthorized actors in person at bank branches throughout the country is just one example of what unauthorized actors can and will do with other Class members' information obtained from the Data Breach. Some of these harms will not materialize for months, or even years after the Data Breach incident, rendering the offer for 12 months of credit monitoring through Kroll by Defendant woefully inadequate to prevent the fraud that will continue to occur through the misuse of Class members' information.

22. Plaintiff Bailey greatly values her privacy in receiving medical services—especially in receiving fertility services—and would not have paid the amount that she did for fertility services if she had known that her information would be maintained using inadequate data security systems.

C. Defendant

23. Defendant ReproSource is a fertility testing company, which operates nationally, including in Rhode Island. ReproSource offers a number of fertility treatment products, including egg supply testing, semen testing, recurrent pregnancy loss laboratory testing services, and other fertility-focused services. ReproSource has a principal place of business at 300 Trade Center, Suite 6540, Woburn, Massachusetts 01801. ReproSource's corporate policies and practices, including those used for data privacy, are established in, and emanate from Massachusetts.

JURISDICTION AND VENUE

24. The Court has jurisdiction over Plaintiffs' claims under 28 U.S.C. § 1332(d)(2), because (a) there are 100 or more Class members, (b) at least one Class member is a citizen of a

state that is diverse from Defendant's citizenship, and (c) the matter in controversy exceeds $5,000,000, exclusive of interest and costs.

25. The Court has personal jurisdiction over Defendant because Defendant's principal place of business is located in this District.

26. Venue is proper in this district under 28 U.S.C. § 1391(b)(1) because Defendant maintains its principal place of business in this District and therefore resides in this District pursuant to 28 U.S.C. § 1391(c)(2). A substantial part of the events or omissions giving rise to the Class's claims also occurred in this District.

FACTS

27. Defendant provides a wide variety of fertility diagnostics to thousands of patients in Rhode Island and hundreds of thousands of patients across the country, as well as providing consultation services to fertility centers. As part of its business, Defendant was entrusted with, and obligated to safeguard and protect the Private Information of, Plaintiffs and the Class in accordance with all applicable laws.

28. In August of 2021, Defendant first learned of an unauthorized entry into its network, which contained customers' Private Information including names, addresses, email addresses, dates of birth, Social Security numbers, financial account numbers, billing, and other health information. Defendant posted the following notice on its website:[1]

> ReproSource is providing notice that it experienced a data security incident in which an unauthorized party may have accessed or acquired protected health information and personally identifiable information of ReproSource patients. This notice explains the steps we have taken to address this issue and additional steps that can be taken to safeguard personal information that was potentially accessed. This notice also explains the incident and offers assistance for individuals whose personal information may have been

[1] *Notice of Data Breach*, (Aug. 8, 2021), https://www.reprosource.com/wp-content/uploads/2021/10/ReproSource-Notice-of-data-breach-10-8-21.pdf [hereinafter *Data Breach Notice*].

accessed, including complimentary credit and identity monitoring services.

What Happened

On August 8, 2021, an unauthorized party accessed the ReproSource network. We discovered ransomware on the morning of August 10, and in less than an hour we severed all network connection activity and contained the incident. We immediately launched a comprehensive investigation to determine the cause and scope of the incident. We retained leading cybersecurity experts to assist with our investigation, confirmed containment of the ransomware, and quickly and securely recovered operations. Additionally, we promptly notified law enforcement.

While our investigation did not confirm that the unauthorized party acquired data in the incident, out of an abundance of caution, we are notifying individuals whose personal information may have been accessed.

We undertook an extensive analysis of our files to determine which data may have been accessed for which individuals and on September 24, 2021, we identified individuals whose data was potentially accessed. Although our data analysis is ongoing, in the interest of initiating notifications, we are in the process of informing individuals whose personal information may have been accessed and we have begun providing the services outlined in this letter.

What Information Was Involved

Based on our analysis to date, personal information in files that may have been accessed or acquired without authorization included: names, addresses, phone numbers, email addresses, dates of birth, billing and health information, such as CPT codes, diagnosis codes, test requisitions and results, test reports and/or medical history information, health insurance or group plan identification names and numbers, and other information provided by individuals or by treating physicians. For a small group of individuals, personal information may have included driver's license numbers, passport numbers, Social Security numbers, financial account numbers, and/or credit card numbers. As previously noted, our data analysis to determine which of the above personal information may have been accessed for which individuals is ongoing.

What We Are Doing

As discussed above, upon learning of the attack, we immediately severed all network connection activity and contained the incident. We promptly notified law enforcement. We also enhanced our cybersecurity by adding additional monitoring and detection tools as additional safeguards against ransomware and other cyber threats.

What You Can Do

To help relieve any concerns you may have following this incident, we have secured the services of Kroll to provide credit and identity monitoring at no cost to those whose personal information may have been accessed, as described in your letter. Kroll is a global leader in risk mitigation and response, and their team has extensive experience helping people who have sustained an unintentional exposure of confidential data. Identity monitoring services that are offered include Credit Monitoring, a Current Credit Report, Web Watcher, Public Persona, Quick Cash Scan, $1 Million Identity Fraud Loss Reimbursement, Fraud Consultation, and Identity Theft Restoration. For further details and to take advantage of this service, please call 1-855-732-0717, Monday through Friday from 8:00 a.m. to 5:30 p.m. Central Time.

Please review the "Additional Resources" section included with this letter below. This section describes additional steps you can take to help protect your information, including recommendations by the Federal Trade Commission regarding identity theft protection and details on how to place a fraud alert or a security freeze on your credit file.

More Information

ReproSource is committed to protecting the privacy of personal information. We will continue to review our physical and electronic safeguards to protect personal information and take appropriate steps to safeguard patient information and our systems.

We deeply regret any inconvenience or concern this may have caused. If you have questions, please call 1-855-732-0717, Monday through Friday from 8:00 a.m. to 5:30 p.m. Central Time with questions.

29. Upon learning of the Data Breach in August 2021, Defendant investigated and estimates that the Private Information of at least 350,000 patients stemming from services previously received was potentially compromised as a result of the Data Breach.[2]

30. In October of 2021, Defendant first announced that it learned of suspicious activity that allowed one or more cybercriminals to access its systems through a ransomware attack. The October, 2021 Notice disclosed that a ransomware attack enabled a threat actor to access ReproSource systems.

31. Defendant offered no explanation for the delay between the initial discovery of the Breach and the belated notification to affected customers, which resulted in Plaintiffs and Class members suffering harm they otherwise could have avoided had a timely disclosure been made.

32. Defendant's delay in notifying its customers affected by the Data Breach violated the provisions of Massachusetts General Laws, Chapter 93H, and in particular the reporting provisions of c. 93H, § 3, which required Defendant, once it knew or had reason to know of a data security breach involving personal information and affecting Massachusetts residents, to provide prompt and direct notice of such breach to any affected Massachusetts residents, to the Massachusetts attorney general, and to the director of consumer affairs and business regulation for Massachusetts.

33. ReproSource's notice of Data Breach was not just untimely but woefully deficient, failing to provide basic details, including but not limited to, how unauthorized parties accessed its networks, whether the information was encrypted or otherwise protected, how it learned of the Data Breach, whether the breach occurred system-wide, whether servers storing information were

[2] These numbers were reported to the Health and Human Services Healthcare Data Breach Portal. *See Cases Currently Under Investigation*, U.S. DEP'T OF HEALTH & HUMAN SERVS.: BREACH PORTAL, https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf [hereinafter *Breach Portal*] (last visited Nov. 8, 2021).

accessed, and how many patients were affected by the Data Breach. Even worse, ReproSource offered only one year of identity monitoring to Plaintiffs and Class members, which required the disclosure of additional PII that ReproSource had just demonstrated it could not be trusted with.

34. Importantly, in an SEC filing by Quest Diagnostics, Inc. (ReproSource's parent company), Quest Diagnostics, Inc. admitted that an unauthorized actor accessed and was able to view the sensitive information of approximately 350,000 of ReproSource's past and present patients as a result of the ransomware attack that affected Plaintiffs' PII.[3]

35. In light of the fraudulent misuse of the PII at issue that has already been committed, it can be determined that Plaintiffs' and Class members' PII is being sold on the dark web, meaning that unauthorized parties have accessed, viewed, and exfiltrated Plaintiffs' and Class members' unencrypted, unredacted, sensitive personal information, including names, addresses, email addresses, dates of birth, Social Security numbers, member ID numbers, policyholder names, employer names, policy numbers, and more.

36. The Breach occurred because Defendant failed to take reasonable measures to protect the PII it collected and stored. Among other things, Defendant failed to implement data security measures designed to prevent this attack, despite repeated warnings to the healthcare industry, insurance companies, and associated entities about the risk of cyberattacks and the highly publicized occurrence of many similar attacks in the recent past on other healthcare providers.

37. Defendant disregarded the rights of Plaintiffs and Class members by intentionally, willfully, recklessly, or negligently failing to take and implement adequate and reasonable measures to ensure that Plaintiffs' and Class members' PII was safeguarded, failing to take

[3] *See* Quest Diagnostics, *SEC Filing Details: Form 8-K* (Oct. 8, 2021), https://ir.questdiagnostics.com/financial-info/sec-filings/sec-filings-details/default.aspx?FilingId=15274830 (last visited Feb. 8, 2022) ("Based on its analysis to date, ReproSource estimates that data accessed may contain personal information of approximately 350,000 patients.")

available steps to prevent an unauthorized disclosure of data, and failing to follow applicable, required and appropriate protocols, policies and procedures regarding the encryption of data, even for internal use. As a result, the PII of Plaintiffs and Class members was compromised through unauthorized access by an unknown third party. Plaintiffs and Class members have a continuing interest in ensuring that their information is and remains safe.

A. Defendant's Privacy Promises

38. ReproSource made, and continues to make, various promises to its customers, including Plaintiffs, that it will maintain the security and privacy of their Private Information.

39. In its Notice of Privacy Practices, which was updated for 2021, and therefore applicable to Plaintiffs, Defendant stated under a section bolded and titled "Our Responsibilities," the following:

- "ReproSource is required by law to maintain the privacy of your PHI."
- "We are required to notify affected individuals in the event of a breach involving unsecured protected health information."
- "We are required to follow the terms of this Notice currently in effect."
- "We need your written authorization to use or disclose your health information for any purpose not covered by the [enumerated categories] below."

40. ReproSource describes how it may use and disclose medical information for each category of uses or disclosures, none of which provide it a right to expose patients' Private Information in the manner in which it was exposed to unauthorized third parties in the Data Breach.

41. By failing to protect Plaintiffs' and Class members' Private Information, and by allowing the Data Breach to occur, ReproSource broke these promises to Plaintiffs and Class members.

B. Defendant Failed to Maintain Reasonable and Adequate Security Measures to Safeguard Customers' Private Information

42. ReproSource acquires, collects, and stores a massive amount of its customers' protected PII, including health information and other personally identifiable data.

43. As a condition of engaging in health-related services, ReproSource requires that patients entrust them with highly confidential Private Information.

44. By obtaining, collecting, using, and deriving a benefit from Plaintiffs' and Class members' Private Information, ReproSource assumed legal and equitable duties and knew or should have known that it was responsible for protecting Plaintiffs' and Class members' Private Information from disclosure.

45. Defendant had obligations created by the Health Insurance Portability and Accountability Act (42 U.S.C. § 1320d *et seq.*) ("HIPAA"), Massachusetts law (including M.G.L., c. 111, §70E(b)), industry standards, common law, and representations made to Class members, to keep Class members' Private Information confidential and to protect it from unauthorized access and disclosure.

46. Defendant failed to properly safeguard Class members' Private Information, allowing hackers to access their Private Information.

47. Plaintiffs and Class members provided their Private Information to Defendant with the reasonable expectation and mutual understanding that Defendant and any of its affiliates would comply with their obligation to keep such information confidential and secure from unauthorized access.

48. Prior to and during the Data Breach, Defendant promised customers that their Private Information would be kept confidential.

49. Defendant's failure to provide adequate security measures to safeguard customers' Private Information is especially egregious because Defendant operates in a field which has recently been a frequent target of scammers attempting to fraudulently gain access to customers' highly confidential Private Information.

50. In fact, Defendant has been on notice for years that the healthcare industry and health insurance companies are a prime target for scammers because of the amount of confidential customer information maintained.

51. Defendant was also on notice that the FBI has been concerned about data security in the healthcare industry. In August 2014, after a cyberattack on Community Health Systems, Inc., the FBI warned companies within the healthcare industry that hackers were targeting them. The warning stated that "[t]he FBI has observed malicious actors targeting healthcare related systems, perhaps for the purpose of obtaining the Protected Healthcare Information (PHI) and/or Personally Identifiable Information (PII)."[4]

52. The American Medical Association ("AMA") has also warned healthcare companies about the important of protecting their patients' confidential information:

> Cybersecurity is not just a technical issue; it's a patient safety issue. AMA research has revealed that 83% of physicians work in a practice that has experienced some kind of cyberattack. Unfortunately, practices are learning that cyberattacks not only threaten the privacy and security of patients' health and financial information, but also patient access to care.[5]

[4] Jim Finkle, *FBI Warns Healthcare Firms that they are Targeted by Hackers*, REUTERS (Aug. 2014), https://www.reuters.com/article/us-cybersecurity-healthcare-fbi/fbi-warnshealthcare-firms-they-are-targeted-by-hackers-idUSKBN0GK24U20140820.

[5] Andis Robeznieks, *Cybersecurity: Ransomware attacks shut down clinics, hospitals*, AM. MED. ASS'N (Oct. 4, 2019), https://www.ama-assn.org/practice-management/sustainability/cybersecurity-ransomware-attacks-shut-down-clinics-hospitals.

53. The number of US data breaches surpassed 1,000 in 2016, a record high and a forty percent increase in the number of data breaches from the previous year.[6] In 2017, a new record high of 1,579 breaches were reported—representing a 44.7 percent increase.[7] That trend continues.

54. The healthcare sector reported the second largest number of breaches among all measured sectors in 2018, with the highest rate of exposure per breach.[8] 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.[9] 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.[10]

55. A 2017 study conducted by HIMSS Analytics showed that email was the most likely cause of a data breach, with 78 percent of providers stating that they experienced a healthcare ransomware or malware attack in the past 12 months.

56. Healthcare related data breaches continued to rapidly increase into 2021 when ReproSource was breached.[11]

---

[6] Identity Theft Resource Center, *Data Breaches Increase 40 Percent in 2016, Finds New Report From Identity Theft Resource Center and CyberScout* (Jan. 19, 2017), https://www.idtheftcenter.org/surveys-studys.
[7] Identity Theft Resource Center, *2017 Annual Data Breach Year-End Review*, https://www.idtheftcenter.org/2017-data-breaches/.
[8] Identity Theft Resource Center, *2018 End -of-Year Data Breach Report*, https://www.idtheftcenter.org/2018-data-breaches/.
[9] Elinor Mills, *Study: Medical identity theft is costly for victims*, CNET (March 3, 2010), https://www.cnet.com/news/study-medical-identity-theft-is-costly-for- victims/.
[10] *Id.*
[11] *2019 HIMSS Cybersecurity Survey*, https://www.himss.org/2019-himsscybersecurity-survey.

57. In the Healthcare industry, the number one threat vector from a cyber security standpoint is phishing. Cybersecurity firm Proofpoint reports that "phishing is the initial point of compromise in most significant [healthcare] security incidents, according to a recent report from the Healthcare Information and Management Systems Society (HIMSS). And yet, 18% of healthcare organizations fail to conduct phishing tests, a finding HIMSS describes as "incredible."[12]

58. As explained by the Federal Bureau of Investigation, "[p]revention is the most effective defense against ransomware and it is critical to take precaution for protection."[13]

59. To prevent and detect ransomware attacks, including the ransomware attack that resulted in the Data Breach, Defendant could and should have implemented, as recommended by the United States Government, the following measures:

- Implement an awareness and training program. Because end users are targets, employees and individuals should be aware of the threat of ransomware and how it is delivered.
- Enable strong spam filters to prevent phishing emails from reaching the end users and authenticate inbound email using technologies like Sender Policy Framework (SPF), Domain Message Authentication Reporting and Conformance (DMARC), and DomainKeys Identified Mail (DKIM) to prevent email spoofing.
- Scan all incoming and outgoing emails to detect threats and filter executable files from reaching end users.
- Configure firewalls to block access to known malicious IP addresses.
- Patch operating systems, software, and firmware on devices. Consider using a centralized patch management system.

[12] Aaron Jensen, *Healthcare Phishing Statistics: 2019 HIMSS Survey Results*, PROOFPOINT (Mar. 27, 2019), https://www.proofpoint.com/us/security-awareness/post/healthcare-phishingstatistics-2019-himss-survey-results.
[13] *See How to Protect Your Networks from RANSOMWARE*, FBI (2016) https ://www. fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf/view.

- Set anti-virus and anti-malware programs to conduct regular scans automatically.

- Manage the use of privileged accounts based on the principle of least privilege; no users should be assigned administrative access unless absolutely needed; and those with a need for administrator accounts should only use them when necessary.
- Configure access controls—including file, directory, and network share permissions—with least privilege in mind. If a user only needs to read specific files, the user should not have write access to those files, directories, or shares.

- Disable macro scripts from office files transmitted via email. Consider using Office Viewer software to open Microsoft Office files transmitted via email instead of full office suite applications.

- Implement Software Restriction Policies (SRP) or other controls to prevent programs from executing from common ransomware locations, such as temporary folders supporting popular Internet browsers or compression/decompression programs, including the AppData/LocalAppData folder.

- Consider disabling Remote Desktop protocol (RDP) if it is not being used.

- Use application whitelisting, which only allows systems to execute programs known and permitted by security policy.

- Execute operating system environments or specific programs in a virtualized environment.

- Categorize data based on organizational value and implement physical and logical separation of networks and data for different organizational units.

60. To prevent and detect ransomware attacks, including the ransomware attack that resulted in the Data Breach, Defendants could and should have implemented, as recommended by the United States Government, the following measures:

- **Update and patch your computer.** Ensure your applications and operating systems (OSs) have been updated with the latest patches. Vulnerable applications and OSs are the target of most ransomware attacks . . .

- **Use caution with links and when entering website addresses.** Be careful when clicking directly on links in emails, even if the sender appears to be someone you know. Attempt to independently verify website addresses (e.g., contact your organization's helpdesk, search the internet for the sender organization's website or the topic mentioned in the email). Pay attention to the website addresses you click on, as well as those you enter yourself. Malicious website addresses often appear almost identical to legitimate sites, often using a slight variation in spelling or a different domain (e.g., .com instead of .net) . . .

- **Open email attachments with caution.** Be wary of opening email attachments, even from senders you think you know, particularly when attachments are compressed files or ZIP files.

- **Keep your personal information safe.** Check a website's security to ensure the information you submit is encrypted before you provide it . . .

- **Verify email senders.** If you are unsure whether or not an email is legitimate, try to verify the email's legitimacy by contacting the sender directly. Do not click on any links in the email. If possible, use a previous (legitimate) email to ensure the contact information you have for the sender is authentic before you contact them.

- **Inform yourself.** Keep yourself informed about recent cybersecurity threats and up to date on ransomware techniques. You can find information about known phishing attacks on the Anti-Phishing Working Group website. You may also want to sign up for CISA product notifications, which will alert you when a new Alert, Analysis Report, Bulletin, Current Activity, or Tip has been published.

- **Use and maintain preventative software programs.** Install antivirus software, firewalls, and email filters—and keep them updated—to reduce malicious network traffic . . .[14]

[14] *See Security Tip (ST19-001) Protecting Against Ransomware*, CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY (Apr. 11, 2019), https://us-cert.cisa.gov/ncas/tips/ST19-001.

61. To prevent and detect ransomware attacks, including the ransomware attack that resulted in the Data Breach, Defendant could and should have implemented, as recommended by the Microsoft Threat Protection Intelligence Team, the following measures:

- **Secure internet-facing assets**
  - Apply the latest security updates
  - Use threat and vulnerability management
  - Perform regular audit; remove privilege credentials;

- **Thoroughly investigate and remediate alerts**
  - Prioritize and treat commodity malware infections as potential full compromise

- **Include IT Pros in security discussions**
  - Ensure collaboration among [security operations], [security admins], and [information technology] admins to configure servers and other endpoints securely;

- **Build credential hygiene**
  - use [multifactor authentication] or [network level authentication] and use strong, randomized, just-in-time local admin passwords

- **Apply principle of least-privilege**
  - Monitor for adversarial activities
  - Hunt for brute force attempts
  - Monitor for cleanup of Event Logs
  - Analyze logon events

- **Harden infrastructure**
  - Use Windows Defender Firewall
  - Enable tamper protection
  - Enable cloud-delivered protection
  - Turn on attack surface reduction rules and [Antimalware Scan Interface] for Office [Visual Basic for Applications].[15]

[15] *See Human-operated ransomware attacks: A preventable disaster*, MICROSOFT (Mar. 5, 2020), https://www.microsoft.com/security/blog/2020/03/05/human-operated-ransomware-attacks-apreventable-disaster/.

62. These are basic, common-sense email security measures that every business, not only healthcare businesses, should be doing. ReproSource, with its heightened standard of care should be doing even more. But by adequately taking these common-sense measures, ReproSource could have prevented this Data Breach from occurring.

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

64. With respect to training, ReproSource specifically failed to:

- Implement a variety of anti-ransomware training tools, in combination, such as computer-based training, classroom training, monthly newsletters, posters, login alerts, email alerts, and team-based discussions;
- Perform regular training at defined intervals such as bi-annual training and/or monthly security updates; and
- Craft and tailor different approaches to different employees based on their base knowledge about technology and cybersecurity.

65. The PII was also maintained on ReproSpurce's computer system in a condition vulnerable to cyberattacks such as through the infiltration of Defendant's systems through ransomware attacks. The mechanism of the cyberattack and the potential for improper disclosure of Plaintiffs' and Class members' PII was a known risk to ReproSource, and thus ReproSource was on notice that failing to take reasonable steps necessary to secure the PII from those risks left the PII in a vulnerable position.

C. The Monetary Value of Privacy Protections and Private Information

66. The fact that Plaintiffs' and Class members' Private Information was stolen—and has already been egregiously misused to perpetrate identity theft in Plaintiff Bailey's case—means that Class members' information is likely for sale by cybercriminals and will be misused in additional instances in the future.

67. At all relevant times, Defendant was well aware that Private Information it collects from Plaintiffs and Class members is highly sensitive and of significant value to those who would use it for wrongful purposes.

68. Private Information is a valuable commodity to identity thieves. As the FTC recognizes, identity thieves can use this information to commit an array of crimes including identify theft, and medical and financial fraud.[16] Indeed, a robust "cyber black market" exists in which criminals openly post stolen PII including sensitive health information on multiple underground Internet websites, commonly referred to as the dark web.

69. At an FTC public workshop in 2001, then-Commissioner Orson Swindle described the value of a consumer's personal information:

> The use of third party information from public records, information aggregators and even competitors for marketing has become a major facilitator of our retail economy. Even [Federal Reserve] Chairman [Alan] Greenspan suggested here some time ago that it's something on the order of the life blood, the free flow of information.[17]

---

[16] Federal Trade Commission, *Warning Signs of Identity Theft* (Sept. 2018), https://www.consumer.ftc.gov/articles/0271-warning-signs-identity-theft .

[17] *Public Workshop: The Information Marketplace: Merging and Exchanging Consumer Data*, FED. TRADE COMM'N Tr. at 8:2-8 (Mar. 13, 2001), https://www.ftc.gov/sites/default/files/documents/public_events/information-marketplace-merging-and-exchanging-consumer-data/transcript.pdf.

70. Commissioner Swindle's 2001 remarks are even more relevant today, as consumers' personal data functions as a "new form of currency" that supports a $26 Billion per year online advertising industry in the United States.[18]

71. The FTC has also recognized that consumer data is a new (and valuable) form of currency. In an FTC roundtable presentation, another former Commissioner, Pamela Jones Harbour, underscored this point:

> 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.[19]

72. Recognizing the high value that consumers place on their Private Information, many companies now offer consumers an opportunity to sell this information.[20] The idea is to give consumers more power and control over the type of information that they share and who ultimately receives that information. And, by making the transaction transparent, consumers will make a profit from their Private Information. This business has created a new market for the sale and purchase of this valuable data.

73. Consumers place a high value not only on their Private Information, but also on the privacy of that data. Researchers have begun to shed light on how much consumers value their data privacy, and the amount is considerable. Indeed, studies confirm that the average direct financial loss for victims of identity theft in 2014 was $1,349.[21]

---

[18] *See* Julia Angwin & Emily Steel, *Web's Hot New Commodity: Privacy*, The Wall Street Journal (Feb. 28, 2011), http://online.wsj.com/article/SB10001424052748703529004576160764037920274.html [hereinafter *Web's New Hot Commodity*].

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

20 *Web's Hot New Commodity*, *supra* note 17.

21 *See* U.S. Dep't of Justice, *Victims of Identity Theft,* OFFICE OF JUSTICE PROGRAMS: BUREAU OF JUSTICE STATISTICS 1 (Nov. 13, 2017), https://www.bjs.gov/content/pub/pdf/vit14.pdf [hereinafter *Victims of Identity Theft*].

74. The value of Plaintiffs' and Class members' Private Information on the black market is substantial. Sensitive health information can sell for as much as $363.[22] This information 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.

75. 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."[23]

76. The ramifications of ReproSource's failure to keep its patients' Private Information secure are long-lasting and severe. Once Private Information is stolen, fraudulent use of that information and damage to victims may continue for years. Fraudulent activity might not show up for 6 to 12 months or even longer.

77. Approximately 21% of victims do not realize their identify has been compromised until more than two years after it has happened.[24] This gives thieves ample time to seek multiple treatments under the victim's name. Forty percent of consumers found out they were a victim of

[22] Center for Internet Security, *Data Breaches: In the Healthcare Sector*, https://www.cisecurity.org/blog/data-breaches-in-the-healthcare-sector/.
[23] Michael Ollove, *The Rise of Medical Identity Theft in Healthcare*, KAISER (Feb. 7, 2014) https://khn.org/news/rise-of-indentity-theft/.
[24] *See Medical ID Theft Checklist*, IDENTITYFORCE https://www.identityforce.com/blog/medical-id-theft-checklist-2.

medical identity theft only when they received collection letters from creditors for expenses that were incurred in their names.[25]

78. Breaches are particularly serious in healthcare industries. The healthcare sector reported the second largest number of breaches among all measured sectors in 2018, with the highest rate of exposure per breach.[26] Indeed, when compromised, healthcare related data is among the most private 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.[27] Almost 50% of the surveyed victims lost their healthcare coverage as a result of the incident, while nearly 30% said their insurance premiums went up after the event. Forty percent of the victims were never able to resolve their identity theft at all. Seventy-four percent said that the effort to resolve the crime and restore their identity was significant or very significant. Data breaches and identity theft have a crippling effect on individuals and detrimentally impact the economy as a whole.[28]

79. At all relevant times, Defendant was well-aware, or reasonably should have been aware, that the Private Information it maintains is highly sensitive and could be used for wrongful purposes by third parties, such as identity theft and fraud. Defendant should have particularly been aware of these risks, given the significant number of data breaches affecting the health care industry and related industries.

---

[25] *The Potential Damages and Consequences of Medical Identify Theft and Healthcare Data Breaches*, EXPERIAN, (Apr. 2010), https://www.experian.com/assets/data-breach/white-papers/consequences-medical-id-theft-healthcare.pdf.

[26] Identity Theft Resource Center, *2018 End-of-Year Data Breach Report*, (2019) https://www.idtheftcenter.org/wp-content/uploads/2019/02/ITRC_2018-End-of-Year-Aftermath_FINAL_V2_combinedWEB.pdf.

[27] Elinor Mills, *Study: Medical identity theft is costly for victims*, CNET (March 3, 2010), https://www.cnet.com/news/study-medical-identity-theft-is-costly-for- victims/.

[28] *Id.*

80. Had Defendant remedied the deficiencies in its security systems, followed industry guidelines, and adopted security measures recommended by experts in the field, Defendant would have prevented the ransomware attack into its systems and, ultimately, the theft of its customers' Private Information.

81. The compromised Private Information in the Data Breach is of great value to hackers and thieves and can be used in a variety of ways. Information about, or related to, an individual for which there is a possibility of logical association with other information is of great value to hackers and thieves. Indeed, "there is significant evidence demonstrating that technological advances and the ability to combine disparate pieces of data can lead to identification of a consumer, computer or device even if the individual pieces of data do not constitute PII."[29] For example, different PII elements from various sources may be able to be linked in order to identify an individual, or access additional information about or relating to the individual.[30] Based upon information and belief, the unauthorized parties utilized the Private Information they obtained through the Data Breach to obtain additional information from Plaintiffs and Class members that was misused.

82. In addition, as technology advances, computer programs may scan the Internet with wider scope to create a mosaic of information that may be used to link information to an individual in ways that were not previously possible. This is known as the "mosaic effect."

83. 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

[29] *Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers, Preliminary FTC Staff Report*, FED. TRADE COMM'N 35-38 (Dec. 2010), https://www.ftc.gov/reports/preliminary-ftc-staff-report-protecting-consumer-privacy-era-rapid-change-proposed-framework.

[30] *See id.* (evaluating privacy framework for entities collecting or using consumer data with can be "reasonably linked to a specific consumer, computer, or other device").

to access users' other accounts. Thus, even if payment card information were not involved in the Data Breach, the unauthorized parties could use Plaintiffs' and Class members' Private Information to access accounts, including, but not limited to email accounts and financial accounts, to engage in the fraudulent activity identified by Plaintiffs.

84. Given these facts, any company that transacts business with customers and then compromises the privacy of customers' Private Information has thus deprived customers of the full monetary value of their transaction with the company.

85. Acknowledging the damage to Plaintiffs and Class members, Defendant instructed customers like Plaintiffs to "remain vigilant by reviewing account statements and monitoring your credit report for unauthorized activity, especially activity that may indicate fraud and identity theft." Plaintiffs and the other Class members now face a greater risk of identity theft.

86. In short, the Private Information exposed is of great value to hackers and cyber criminals and the data compromised in the Data Breach can be used in a variety of unlawful manners, including opening new credit and financial accounts in users' names.

D. ReproSource's Conduct violated HIPPA

87. HIPAA requires covered entities like ReproSource protect against reasonably anticipated threats to the security of PHI. Covered entities must implement safeguards to ensure the confidentiality, integrity, and availability of PHI. Safeguards must include physical, technical, and administrative components.[31]

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

[31] *What is Considered Protected Health Information Under HIPAA*?, HIPPA JOURNAL, https://www.hipaajournal.com/what-is-considered-protected-health-information-under-hipaa/.

handling Private Information like the data Defendant left unguarded. The HHS has subsequently promulgated five rules under authority of the Administrative Simplification provisions of HIPAA.

89. The HIPAA Breach Notification Rule, 45 CFR §§ 164.400-414, also required Defendant to provide notice of the breach to each affected individual "without unreasonable delay and in no case later than 60 days following discovery of the breach."[32]

90. Defendant's Data Breach resulted from a combination of insufficiencies that demonstrate Defendant failed to comply with safeguards mandated by HIPAA regulations. ReproSource's security failures include, but are not limited to, the following:

- Failing to ensure the confidentiality and integrity of electronic protected health information that Defendant creates, receives, maintains, and transmits in violation of 45 C.F.R. §164.306(a)(1);
- 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 C.F.R. §164.312(a)(1);
- 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);
- 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 C.F.R. §164.308(a)(6)(ii);
- Failing to protect against any reasonably-anticipated threats or hazards to the security or integrity of electronic protected health information in violation of 45 C.F.R. §164.306(a)(2);
- Failing to protect against any reasonably anticipated uses or disclosures of electronically protected health information that are not permitted under the privacy rules regarding individually

[32] *Breach Notification Rule*, U.S. DEP'T HEALTH & HUMAN SERVS., https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html.

identifiable health information in violation of 45 C.F.R. §164.306(a)(3);

- Failing to ensure compliance with HIPAA security standard rules by their workforce in violation of 45 C.F.R. §164.306(a)(94);

- Impermissibly and improperly using and disclosing protected health information that is and remains accessible to unauthorized persons in violation of 45 C.F.R. §164.502, *et seq.*;

- Failing to effectively train all members of their workforce (including independent contractors) on the policies and procedures with respect to protected health information as necessary and appropriate for the members of their workforce to carry out their functions and to maintain security of protected health information in violation of 45 C.F.R. §164.530(b) and 45 C.F.R. §164.308(a)(5); and

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

E. ReproSource Failed to Comply with FTC Guidelines

91. ReproSource was also prohibited by the Federal Trade Commission Act ("FTC Act") (15 U.S.C. §45) from engaging in "unfair or deceptive acts or practices in or affecting commerce." The Federal Trade Commission ("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 the FTC Act. *See, e.g., FTC v. Wyndham Worldwide Corp*., 799 F.3d 236 (3d Cir. 2015).

92. The FTC has promulgated numerous guides for businesses that 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.[33]

93. In 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which established cybersecurity guidelines for businesses.[34] 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.

94. The FTC further recommends that companies not maintain Private Information longer than is needed for authorization of a transaction; limit access to private 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.[35]

95. 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.

---

[33] *Start With Security: A Guide for Business*, FED. TRADE. COMM'N (June 2015), https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf [hereinafter *Start with Security*].

[34] *Protecting Personal Information: A Guide for Business*, FED. TRADE. COMM'M (Oct. 2016), https://www.ftc.gov/system/files/documents/plain-language/pdf- 0136_proteting-personal-information.pdf.

[35] *Start with Security*, *supra* note 32.

96. ReproSource was at all times fully aware of its obligation to protect the Private Information of patients because of its position as a trusted healthcare provider. ReproSource was also aware of the significant repercussions that would result from its failure to do so.

F. ReproSource Failed to Comply with Healthcare Industry Standards

97. HHS's Office for Civil Rights has stated:

> While all organizations need to implement policies, procedures, and technical solutions to make it harder for hackers to gain access to their systems and data, this is especially important in the healthcare industry. Hackers are actively targeting healthcare organizations, as they store large quantities of highly Private and valuable data.[36]

98. HHS highlights several basic cybersecurity safeguards that can be implemented to improve cyber resilience that require a relatively small financial investment yet can have a major impact on an organization's cybersecurity posture including: (a) the proper encryption of Private Information; (b) educating and training healthcare employees on how to protect Private Information; and (c) correcting the configuration of software and network devices.

99. Private cybersecurity firms have also identified the healthcare sector as being particularly vulnerable to cyber-attacks, both because the of the value of the Private Information which they maintain and because as an industry they have been slow to adapt and respond to cybersecurity threats.[37] They too have promulgated similar best practices for bolstering cybersecurity and protecting against the unauthorized disclosure of Private Information.

100. Despite the abundance and availability of information regarding cybersecurity best practices for the healthcare industry, ReproSource chose to ignore them. These best practices were

[36] *Cybersecurity Best Practices for Healthcare Organizations*, HIPAA JOURNAL (Nov. 1, 2018), https://www.hipaajournal.com/important-cybersecurity-best-practices-for-healthcare-organizations/.

[37] *See, e.g.*, *10 Best Practices For Healthcare Security*, INFOSEC, https://resources.infosecinstitute.com/topics/healthcare-information-security/#gref.

known, or should have been known by ReproSource, whose failure to heed and properly implement them directly led to the Data Breach and the unlawful exposure of Private Information.

G. Damages to Plaintiffs and the Class

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

102. The ramifications of ReproSource's failure to keep patients' Private Information secure are long lasting and severe. Once Private Information is stolen, fraudulent use of that information and damage to the victims may continue for years. Consumer victims of data breaches are more likely to become victims of identity fraud.[38]

103. In addition to their obligations under state and federal laws and regulations, Defendant owed a common law duty to Plaintiffs and Class members to protect Private Information entrusted to it, including 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 parties.

104. Defendant further owed and breached its duty to Plaintiffs and Class members to implement processes and specifications that would detect a breach of its security systems in a timely manner and to timely act upon warnings and alerts, including those generated by its own security systems.

105. As a direct result of Defendant's intentional, willful, reckless, and negligent conduct which resulted in the Data Breach, unauthorized parties were able to access, acquire, view, publicize, and/or otherwise commit the identity theft and misuse of Plaintiffs' and Class members'

[38] *2014 LexisNexis True Cost of Fraud Study*, LEXISNEXIS (Aug. 2014), https://www.lexisnexis.com/risk/downloads/assets/true-cost-fraud-2014.pdf.

Private Information as detailed above, and Plaintiffs and members of the Class are now at a heightened and increased substantial risk of identity theft and fraud.

106. The risks associated with identity theft are serious. While some identity theft victims can resolve their problems quickly, others spend hundreds to thousands of dollars and many days repairing damage to their good name and credit record. Some consumers victimized by identity theft may lose out on job opportunities, or be denied loans for education, housing or cars because of negative information on their credit reports. In rare cases, they may even be arrested for crimes they did not commit.

107. Some of the injuries and risks associated with the loss of personal information have already manifested themselves in Plaintiffs' lives. Plaintiff Bickham received a cryptically written notice letter from Defendant stating that her information was released, and that she should remain vigilant for fraudulent activity on her accounts, with no other explanation of where this information could have gone, or who might have access to it. Plaintiff Bickham has already spent hours on the phone trying to determine what negative effects may occur from the loss of her personal information and now faces a certainly impending and substantial risk of a slew of future harms, in light of the fact that the PII has already been fraudulently misused.

108. In addition to this impending risk and having to now spend time on the phone with representatives from ReproSource and constantly monitor her credit accounts, Plaintiff Bickham has also decided to forgo further treatment at facilities that use ReproSource services. Plaintiff Bickham values her privacy but would consider returning to do business with ReproSource if it made substantive and meaningful improvements to its data security practices.

109. In Plaintiff Bailey's case, the compromise of her PII has already caused her to become a victim of identity theft twice since the Data Breach, with unauthorized actors using

information that would have been available on Defendant's systems to steal her identity and take out loans in her name.

110. Plaintiffs and the Class have suffered or face a substantial risk of suffering out-of-pocket fraud losses such as fraudulent charges on online accounts, credit card fraud, loans opened in their names, medical services billed in their names, and identity theft.

111. Plaintiffs and Class members have, may have, and/or will have incurred out of pocket costs for protective measures such as credit monitoring fees, credit report fees, credit freeze fees, and similar costs directly or indirectly related to the Data Breach.

112. Plaintiffs and Class members did not receive the full benefit of their bargain with ReproSource, and instead received services that were of a diminished value to those described in their agreements with ReproSource. They were damaged in an amount at least equal to the difference in the value between the services they thought they paid for (which would have included adequate data security protection) and the services they actually received.

113. Plaintiffs and Class members would not have obtained services from Defendant had Defendant told them that it failed to properly train its employees, lacked safety controls over its computer network, and did not have proper data security practices to safeguard their Private Information from criminal theft and misuse.

114. Due to the already-realized fraudulent misuse of the compromised PII, Plaintiffs and the Class will continue to spend significant amounts of time to monitor their financial and medical accounts for misuse.

115. The theft of Social Security Numbers, which were purloined as part of the Data Breach, is particularly detrimental to victims. The U.S. Social Security Administration ("SSA")

warns that "[i]dentity theft is one of the fastest growing crimes in America."[39] The SSA has stated that "[i]dentity thieves can use your number and your good credit to apply for more credit in your name. Then, they use the credit cards and don't pay the bills, it damages your credit. You may not find out that someone is using your number until you're turned down for credit, or you begin to get calls from unknown creditors demanding payment for items you never bought."[40] In short, "[s]omeone illegally using your Social Security number and assuming your identity can cause a lot of problems."[41]

116. In fact, a new Social Security number is substantially less effective where "other personal information, such as [the victim's] name and address, remains the same" and for some victims, "a new number actually creates new problems. If the old credit information is not associated with your new number, the absence of any credit history under your new number may make it more difficult for you to get credit."[42]

117. Identity thieves can use the victim's Private Information to commit any number of frauds, such as obtaining a job, procuring housing, or even giving false information to police during an arrest. In the healthcare industry context, Private Information can be used to submit false insurance claims. As a result, Plaintiffs and Class members now face a real and continuing immediate risk of identity theft and other problems associated with the disclosure of their Social Security numbers and will need to monitor their credit for an indefinite duration. For Plaintiffs and Class members, this risk creates unending feelings of fear and annoyance. Private information is especially valuable to identity thieves. Defendant knew or should have known this and

39 *Identity Theft And Your Social Security Number*, SOCIAL SECURITY ADMIN. (Dec. 2013), http://www.ssa.gov/pubs/EN-05-10064.pdf.
40 *Id.*
41 *Id.*
42 *Id.*

strengthened its data systems accordingly. Defendant was put on notice of the substantial and foreseeable risk of harm from a data breach, yet it failed to properly prepare for that risk.

118. As a result of the Data Breach, Plaintiffs' and Class members' Private Information has diminished in value.

119. The Private Information belonging to Plaintiffs and Class members is private and was left inadequately protected by Defendant who did not obtain Plaintiffs' or Class members' consent to disclose such Private Information to any other person as required by applicable law and industry standards. Defendant disclosed information about Plaintiffs and the Class that was of an extremely personal and sensitive nature as a direct result of its inadequate security measures.

120. The Data Breach was a direct and proximate result of Defendant's failure to: (a) properly safeguard and protect Plaintiffs' and Class members' Private Information from unauthorized access, use, and disclosure, as required by various state and federal regulations, industry practices, and common law; (b) establish and implement appropriate administrative, technical, and physical safeguards to ensure the security and confidentiality of Plaintiffs' and Class members' Private Information; and (c) protect against reasonably foreseeable threats to the security or integrity of such information.

121. Defendant had the resources necessary to prevent the Data Breach, but neglected to adequately implement data security measures, despite its obligation to protect customer data.

122. Defendant did not properly train its employees to identify and avoid ransomware attacks.

123. Had Defendant remedied the deficiencies in its data security systems and adopted security measures recommended by experts in the field, it would have prevented the intrusions into its systems and, ultimately, the theft of Plaintiffs' and Class members' Private Information.

124. As a direct and proximate result of Defendant's wrongful actions and inactions, Plaintiffs and Class members have been placed at an imminent, immediate, and continuing increased risk of harm from identity theft and fraud, requiring them to take the time which they otherwise would have dedicated to other life demands such as work and family in an effort to mitigate the actual and potential impact of the Data Breach on their lives.

125. The U.S. Department of Justice's Bureau of Justice Statistics found that "among victims who had personal information used for fraudulent purposes, twenty-nine percent spent a month or more resolving problems" and that "resolving the problems caused by identity theft [could] take more than a year for some victims."[43]

126. Other than offering 12 months of credit monitoring, Defendant did not take any measures to assist Plaintiffs and Class members other than telling them to simply do the following:

- remain vigilant for incidents of fraud and identity theft;
- review account statements and monitor credit reports for unauthorized activity;
- obtain a copy of free credit reports;
- contact the FTC and/or the state Attorney General's office;
- enact a security freeze on credit files; and
- create a fraud alert.

None of these recommendations, however, require Defendant to expend any effort to protect Plaintiffs' and Class members' Private Information.

127. Defendant's failure to adequately protect Plaintiffs and Class members' Private Information has resulted in Plaintiffs and Class members having to undertake these tasks, which

[43] *See* U.S. Dep't of Justice, *Victims of Identity Theft,* OFFICE OF JUSTICE PROGRAMS: BUREAU OF JUSTICE STATISTICS 1 (Nov. 13, 2017), https://www.bjs.gov/content/pub/pdf/vit14.pdf [hereinafter *Victims of Identity Theft*].

require extensive amounts of time, calls, and, for many of the credit and fraud protection services, payment of money–while Defendant sits by and does nothing to assist those affected by the incident. Instead, as ReproSource's Data Breach Notice indicates, it is putting the burden on Plaintiffs and Class members to discover possible fraudulent activity and identity theft.

128. While Defendant offered one year of credit monitoring, the credit monitoring offered from Kroll does not guarantee privacy or data security for Plaintiffs. Thus, to mitigate harm, Plaintiffs and Class members are now burdened with indefinite monitoring and vigilance of their accounts.

129. Moreover, the offer of 12 months of identity monitoring to Plaintiffs and Class members is woefully inadequate. While some harm has already taken place, including the fraudulent misuse of the compromised PII, the worst is yet to come. There may be a time lag between when harm occurs versus when it is discovered, and between when Private Information is acquired and when it is used. Furthermore, identity theft monitoring only alerts someone to the fact that they have already been the victim of identity theft (*i.e.*, fraudulent acquisition and use of another person's Private Information) – it does not prevent identity theft.[44] This is especially true for many kinds of medical identity theft, for which most credit monitoring plans provide little or no monitoring or protection.

130. Plaintiffs and Class members have been damaged in several other ways as well. Plaintiffs and Class members have been exposed to an impending, imminent, and ongoing increased risk of fraud, identity theft, and other misuse of their Private Information. Plaintiffs and Class members must now and indefinitely closely monitor their financial and other accounts to

[44] *See, e.g.*, Kayleigh Kulp, *Credit Monitoring Services May Not Be Worth the Cost*, CNBC (Nov. 30, 2017), https://www.cnbc.com/2017/11/29/credit-monitoring-services-may-not-beworth-the-cost.html.

guard against fraud. This is a burdensome and time-consuming task. Plaintiffs and Class members have also been forced to purchase adequate credit reports, credit monitoring and other identity protection services, and have placed credit freezes and fraud alerts on their credit reports, while also spending significant time investigating and disputing fraudulent or suspicious activity on their accounts. Plaintiffs and Class members also suffered a loss of the inherent value of their Private Information.

131. The Private Information stolen in the Data Breach can be misused on its own or can be combined with personal information from other sources such as publicly available information, social media, etc. to create a package of information capable of being used to commit further identity theft. Thieves can also use the stolen Private Information to send spear-phishing emails to Class members to trick them into revealing sensitive information. Lulled by a false sense of trust and familiarity from a seemingly valid sender (for example Wells Fargo, Amazon, or a government entity), the individual agrees to provide sensitive information requested in the email, such as login credentials, account numbers, and the like.

132. As a result of Defendant's failures to prevent the Data Breach, Plaintiffs and Class members have suffered, will suffer, and are at increased risk of suffering:

- The compromise, publication, theft and/or unauthorized use of their Private Information;
- Out-of-pocket costs associated with the prevention, detection, recovery and remediation from identity theft or fraud;
- Lost opportunity costs and lost wages associated with efforts expended and the loss of productivity from 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 and fraud;

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

- Current and future costs in terms of time, effort and money that will be expended to prevent, detect, contest, remediate and repair the impact of the Data Breach for the remainder of the lives of Plaintiffs and Class members; and

- Anxiety and distress resulting fear of misuse of their Private Information.

133. In addition to a remedy for the economic harm, Plaintiffs and Class members maintain an undeniable interest in ensuring that their Private Information remains secure and is not subject to further misappropriation and theft.

CLASS ACTION ALLEGATIONS

134. Plaintiffs bring 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), 23(b)(3), and/or 23(c)(4).

135. Specifically, Plaintiffs propose the following Nationwide Class and Rhode Island and North Carolina Subclasses (collectively, the "Class") definitions:

Nationwide Class
All persons residing in the United States whose Private Information was compromised as a result of the Data Breach discovered on or about August 10, 2021 and who were sent notice of the Data Breach.

Rhode Island Subclass
All persons residing in Rhode Island whose Private Information was compromised as a result of the Data Breach discovered on or about August 10, 2021 and who were sent notice of the Data Breach.

North Carolina Subclass
All persons residing in North Carolina whose Private Information was compromised as a result of the Data Breach discovered on or about August 10, 2021 and who were sent notice of the Data Breach.

Excluded from the Class are Defendant and Defendant's affiliates, parents, subsidiaries, employees, officers, agents, and directors. Also excluded are any judicial officers presiding over this matter and the members of their immediate families and judicial staff.

136. Plaintiffs reserve the right to modify, change, amend, or expand the definitions of the Nationwide Class and Subclasses based upon discovery and further investigation.

137. Certification of Plaintiffs' claims for class-wide treatment is appropriate because Plaintiffs can prove the elements of the claims on a class-wide basis using the same evidence as would be used to prove those elements in individual actions alleging the same claims.

138. **Numerosity—Federal Rule of Civil Procedure 23(a)(1).** The members of the Class are so numerous that joinder of all Class members would be impracticable. On information and belief, the Class numbers in the thousands. Moreover, the Class and Subclasses are composed of an easily ascertainable set of individuals and entities who were patients of Defendant and who were impacted by the Data Breach. The precise number of Class members has already been ascertained and can be further confirmed through discovery, which includes Defendant's records. The disposition of Plaintiffs and Class members' claims through a class action will benefit the parties and this Court.

139. **Commonality and Predominance—Federal Rule of Civil Procedure 23(a)(2) and 23(b)(3).** Common questions of law and fact exist as to all members of the Class and predominate over questions affecting only individual members of the Class. Such common questions of law or fact include, *inter alia*:

- Whether Defendant's data security systems prior to and during the Data Breach complied with applicable data security laws and regulations;
- Whether Defendant's data security systems prior to and during the Data Breach were consistent with industry standards;

- Whether Defendant properly implemented its purported security measures to protect Plaintiffs' and the Class's Private Information from unauthorized capture, dissemination, and misuse;

- Whether Defendant took reasonable measures to determine the extent of the Data Breach after it first learned of same;

- Whether Defendant disclosed Plaintiffs' and the Class's Private Information in violation of the understanding that the Private Information was being disclosed in confidence and should be maintained;

- Whether Defendant willfully, recklessly, or negligently failed to maintain and execute reasonable procedures designed to prevent unauthorized access to Plaintiffs' and the Class's Private Information;

- Whether Defendant was negligent in failing to properly secure and protect Plaintiffs' and the Class's Private Information;

- Whether Defendant was unjustly enriched by its actions; and

- Whether Plaintiffs and the other members of the Class are entitled to damages, injunctive relief, or other equitable relief, and the measure of such damages and relief.

140. Defendant engaged in a common course of conduct giving rise to the legal rights sought to be enforced by Plaintiffs, on behalf of themselves and other members of the Class. Similar or identical common law violations, business practices, and injuries are involved. Individual questions, if any, pale by comparison, in both quality and quantity, to the numerous common questions that predominate in this action.

141. **Typicality—Federal Rule of Civil Procedure 23(a)(3).** Plaintiffs' claims are typical of the claims of the other members of the Class because, among other things, all Class members were similarly injured and sustained similar monetary and economic injuries as a result

of Defendant's uniform misconduct described above and were thus all subject to the Data Breach alleged herein. Further, there are no defenses available to Defendant that are unique to Plaintiffs.

142. **Adequacy of Representation—Federal Rule of Civil Procedure 23(a)(4).** Plaintiffs are an adequate representative of the Class because their interests do not conflict with the interests of the Class they seek to represent, they has retained counsel competent and experienced in complex class action litigation, and Plaintiffs will prosecute this action vigorously. The Class's interests will be fairly and adequately protected by Plaintiffs and their counsel.

143. **Injunctive Relief—Federal Rule of Civil Procedure 23(b)(2).** Defendant has acted and/or refused to act on grounds that apply generally to the Class, making injunctive and/or declaratory relief appropriate with respect to the Class under Fed. Civ. P. 23 (b)(2).

144. **Superiority—Federal Rule of Civil Procedure 23(b)(3).** A class action is superior to any other available means 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. The damages or other financial detriment suffered by Plaintiffs and the other members of the Class are relatively small compared to the burden and expense that would be required to individually litigate their claims against Defendant, so it would be impracticable for members of the Class to individually seek redress for Defendant's wrongful conduct. Even if members of the Class could afford individual litigation, the court system could not. Individualized litigation creates a potential for inconsistent or contradictory judgments and increases the delay and expense to all parties and the court system. By contrast, the class action device presents far fewer management difficulties and provides the benefits of a single adjudication, economy of scale, and comprehensive supervision by a single court.

145. Class certification is also appropriate under Rules 23(b)(1) and/or (b)(2) because:

a. The prosecution of separate actions by the individual members of the Class would create a risk of inconsistent or varying adjudications establishing incompatible standards of conduct for Defendant;

b. The prosecution of separate actions by individual Class members would create a risk of adjudication that would, as a practical matter, be dispositive of the interests of other Class members not parties to the adjudications, or would substantially impair or impede their ability to protect their interests; and

c. Defendant has acted and refused to act on grounds generally applicable to the Class, thereby making appropriate final injunctive relief with respect to the members of the Class as a whole.

146. Class certification is also appropriate because this Court can designate particular claims or issues for class-wide treatment and may designate multiple subclasses pursuant to Fed. R. Civ. P. 23(c)(4).

147. No unusual difficulties are likely to be encountered in the management of this action as a class action.

COUNT I
NEGLIGENCE
(On Behalf of Plaintiffs and the Nationwide Class or, Alternatively, the State Subclasses)

148. Plaintiffs fully incorporate by reference all of the above paragraphs, as though fully set forth herein.

149. Upon Defendant's accepting and storing the Private Information of Plaintiffs and the Class in its computer systems and on its networks, Defendant undertook and owed a duty to Plaintiffs and the Class to exercise reasonable care to secure and safeguard that information and to

use commercially reasonable methods to do so. Defendant knew that the Private Information was private and confidential and should be protected as private and confidential.

150. Defendant owed a duty of care not to subject Plaintiffs' and the Class's Private Information to an unreasonable risk of exposure and theft because Plaintiffs and the Class were foreseeable and probable victims of any inadequate security practices.

151. Defendant owed numerous duties to Plaintiffs and the Class, including the following:

- to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting and protecting Private Information in its possession;
- to protect Private Information using reasonable and adequate security procedures and systems that are compliant with industry-standard practices; and
- to implement processes to quickly detect a data breach and to timely act on warnings about data breaches.

152. Defendant also breached its duty to Plaintiffs and Class members to adequately protect and safeguard Private Information by disregarding standard information security principles, despite obvious risks, and by allowing unmonitored and unrestricted access to unsecured Private Information. Furthering its dilatory practices, Defendant 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 a malicious third party to gather Plaintiffs' and Class members' Private Information and potentially misuse the Private Information and intentionally disclose it to others without consent.

153. Defendant knew, or should have known, of the risks inherent in collecting and storing Private Information and the importance of adequate security. Defendant knew or should have known about numerous well-publicized data breaches within the medical industry.

154. Defendant knew, or should have known, that its data systems and networks did not adequately safeguard Plaintiffs' and Class members' Private Information.

155. Defendant breached its duties to Plaintiffs and Class members by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiffs' and Class members' Private Information.

156. Because Defendant knew that a breach of its systems would damage thousands of its customers, including Plaintiffs and Class members, Defendant had a duty to adequately protect its data systems and the Private Information contained thereon.

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

158. In addition, Defendant had a duty to employ reasonable security measures under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data.

159. Defendant also had a duty under HIPAA privacy laws, which were enacted with the objective of protecting the confidentiality of clients' healthcare information and set forth the conditions under which such information can be used, and to whom it can be disclosed. HIPAA privacy laws not only apply to healthcare providers and the organizations they work for, but to any entity that may have access to healthcare information about a patient that—if it were to fall into the wrong hands—could present a risk of harm to the patient's finances or reputation.

160. Defendant also had a duty under M.G.L., c. 111, § 70E(b) to ensure that all customers' medical records and communications are kept confidential.

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

162. Defendant's own conduct also created a foreseeable risk of harm to Plaintiffs and Class members and their Private Information. Defendant's misconduct included failing to: (1) secure Plaintiffs' and Class member's Private Information; (2) comply with industry standard security practices; (3) implement adequate system and event monitoring; and (4) implement the systems, policies, and procedures necessary to prevent this type of data breach.

163. Defendant breached its duties, and thus was negligent, by failing to use reasonable measures to protect Class members' Private Information, and by failing to provide timely notice of the Data Breach. 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 Defendant's networks and systems;

c. Allowing unauthorized access to Class members' Private Information;

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

e. 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

164. Through Defendant's acts and omissions described in this Complaint, including its failure to provide adequate security and failure to protect Plaintiffs' and Class members' Private Information from being foreseeably captured, accessed, disseminated, stolen and misused, Defendant unlawfully breached its duty to use reasonable care to adequately protect and secure Plaintiffs' and Class members' Private Information during the time it was within Defendant's possession or control.

165. Defendant's conduct was grossly negligent and departed from all reasonable standards of care, including, but not limited to failing to adequately protect the Private Information and failing to provide Plaintiffs and Class members with timely notice that their sensitive Private Information had been compromised.

166. Neither Plaintiffs nor the other Class members contributed to the Data Breach and subsequent misuse of their Private Information as described in this Complaint.

167. As a direct and proximate result of Defendant's conduct, Plaintiffs and Class members suffered damages as alleged above.

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

COUNT II
BREACH OF CONTRACT
(On Behalf of Plaintiffs and the Nationwide Class or, Alternatively, the State Subclasses)

169. Plaintiffs fully incorporate by reference all of the above paragraphs, as though fully set forth herein.

170. Plaintiffs and other Class members entered into valid and enforceable express contracts with Defendant under which Plaintiffs and other Class members agreed to provide their Private Information to Defendant, and Defendant agreed to provide testing services and, impliedly, if not explicitly, agreed to protect Plaintiffs' and Class members' Private Information.

171. These contracts include HIPAA privacy notices and explanation of benefits documents.

172. To the extent Defendant's obligation to protect Plaintiffs' and other Class members' Private Information was not explicit in those express contracts, the express contracts included implied terms requiring Defendant to implement data security adequate to safeguard and protect the confidentiality of Plaintiffs' and other Class members' Private Information, including in accordance with HIPAA regulations; federal, state and local laws; and industry standards. Neither Plaintiffs nor any Class member would have entered into these contracts with Defendant without understanding that Plaintiffs' and other Class members' Private Information would be safeguarded and protected; stated otherwise, data security was an essential implied term of the parties' express contracts.

173. A meeting of the minds occurred, as Plaintiffs and other Class members agreed, among other things, to provide their Private Information in exchange for Defendant's agreement to protect the confidentiality of that Private Information.

174. The protection of Plaintiffs' and Class members' Private Information were material aspects of Plaintiffs' and Class members' contracts with Defendant.

175. Defendant's promises and representations described above relating to HIPAA and industry practices, and Defendant's purported concern about its clients' privacy rights became terms of the contracts between Defendant and its clients, including Plaintiffs and other Class

members. Defendant breached these promises by failing to comply with HIPAA and reasonable industry practices.

176. Plaintiffs and Class members read, reviewed, and/or relied on statements made by or provided by ReproSource and/or otherwise understood that ReproSource would protect its patients' Private Information if that information were provided to ReproSource.

177. Plaintiffs and Class members fully performed their obligations under the implied contract with Defendant; however, Defendant did not.

178. As a result of Defendant's breach of these terms, Plaintiffs and other Class members have suffered a variety of damages including but not limited to: the lost value of their privacy; not getting the benefit of their bargain with Defendant; the lost difference in the value between the secure health services Defendant promised and the insecure services received; the value of the lost time and effort required to mitigate the actual and potential impact of the Data Breach on their lives, including, *inter alia*, that required to place "freezes" and "alerts" with credit reporting agencies, to contact financial institutions, to close or modify financial and medical accounts, to closely review and monitor credit reports and various accounts for unauthorized activity, and to file police reports; and Plaintiffs and other Class members have been put at increased risk of future identity theft, fraud, and/or misuse of their Private Information, which may take years to manifest, discover, and detect.

179. Plaintiffs and Class members are therefore entitled to damages, including restitution and unjust enrichment, disgorgement, declaratory and injunctive relief, and attorney fees, costs, and expenses.

COUNT III
BREACH OF IMPLIED CONTRACT
(On Behalf of Plaintiffs and the Nationwide Class or, Alternatively, the State Subclasses)

180. Plaintiffs fully incorporate by reference all of the above paragraphs, as though fully set forth herein.

181. Plaintiffs bring this claim for breach of implied contract in the alternative to their breach of contract claim.

182. Through their course of conduct, Defendant, Plaintiffs, and Class members entered into implied contracts for the provision of healthcare services, as well as implied contracts for the Defendant to implement data security adequate to safeguard and protect the privacy of Plaintiffs' and Class members' Private Information.

183. Specifically, Plaintiffs entered into a valid and enforceable implied contract with Defendant when they first entered into the testing services agreement with Defendant.

184. The valid and enforceable implied contracts to provide fertility services that Plaintiffs and Class members entered into with Defendant include Defendant's promise to protect nonpublic Private Information given to Defendant or that Defendant created on its own from disclosure.

185. When Plaintiffs and Class members provided their Private Information to Defendant in exchange for Defendant's services, they entered into implied contracts with Defendant pursuant to which Defendant agreed to reasonably protect such information.

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

187. In entering into such implied contracts, Plaintiffs and Class members reasonably believed and expected that Defendant's data security practices complied with relevant laws and regulations and were consistent with industry standards.

188. Class members who paid money to Defendant reasonably believed and expected that Defendant would use part of those funds to obtain adequate data security. Defendant failed to do so.

189. Under implied contracts, Defendant and/or its affiliated providers promised and were obligated to: (a) provide fertility services to Plaintiffs and Class members; and (b) protect Plaintiffs' and Class members' Private Information provided to obtain the benefits of such services. In exchange, Plaintiffs and Members of the Class agreed to pay money for these services, and to turn over their Private Information.

190. Both the provision of testing services and the protection of Plaintiffs' and Class members' Private Information were material aspects of these implied contracts.

191. The implied contracts for the provision of fertility testing services—contracts that include the contractual obligations to maintain the privacy of Plaintiffs' and Class members' Private Information—are also acknowledged, memorialized, and embodied in multiple documents, including (among other documents) Defendant's Data Breach notification letter and Defendant's Notice of Privacy Practices.

192. Defendant's express representations, including, but not limited to the express representations found in its Notice of Privacy Practices, memorializes and embodies the implied contractual obligation requiring Defendant to implement data security adequate to safeguard and protect the privacy of Plaintiffs' and Class members' Private Information.

193. Consumers of fertility testing services value their privacy, the privacy of their dependents, and the ability to keep confidential their Private Information associated with obtaining such services. Plaintiffs and Class members would not have entrusted their Private Information to Defendant and entered into these implied contracts with Defendant without an understanding that their Private Information would be safeguarded and protected, nor would they have entrusted their Private Information to Defendant in the absence of its implied promise to monitor its computer systems and networks to ensure that it adopted reasonable data security measures.

194. A meeting of the minds occurred, as Plaintiffs and Class members agreed and provided their Private Information to Defendant and/or its affiliated healthcare providers and paid for the provided testing services in exchange for, among other things, both the provision of healthcare and the protection of their Private Information.

195. Plaintiffs and Class members performed their obligations under the contract when they paid for Defendant's services and provided their Private Information.

196. Defendant materially breached its contractual obligation to protect the nonpublic Private Information Defendant gathered when the information was accessed and exfiltrated by the Data Breach.

197. Defendant materially breached the terms of the implied contracts, including, but not limited to, the terms stated in the relevant Notice of Privacy Practices. Defendant did not maintain the privacy of Plaintiffs' and Class members' Private Information as evidenced by its notifications of the Data Breach to Plaintiffs and Class members. Specifically, Defendant did not comply with industry standards, standards of conduct embodied in statutes like Section 5 of the FTCA, or otherwise protect Plaintiffs' and Class members' private information as set forth above.

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

199. As a result of Defendant's failure to fulfill the data security protections promised in these contracts, Plaintiffs and Class members did not receive full benefit of the bargain, and instead received healthcare and other services that were of a diminished value to that described in the contracts. Plaintiffs and Class members, therefore, were damaged in an amount at least equal to the difference in the value between the healthcare with data security protection they paid for and the healthcare they received.

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

201. As a direct and proximate result of the Data Breach, Plaintiffs and Class members have been harmed and suffered, and will continue to suffer, actual damages and injuries, including without limitation the release and disclosure of their Private Information, the loss of control of their Private Information, the imminent risk of suffering additional damages in the future, disruption of their medical care and treatment, out of pocket expenses, and the loss of the benefit of the bargain they had struck with Defendant.

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

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

COUNT IV
BREACH OF FIDUCIARY DUTY
(On Behalf of Plaintiffs and the Nationwide Class or, Alternatively, the State Subclasses)

204. Plaintiffs fully incorporate by reference all of the above paragraphs, as though fully set forth herein.

205. In providing their Private Information to Defendant, Plaintiffs and Class members justifiably placed a special confidence in Defendant to act in good faith and with due regard for the interests of Plaintiffs and Class members to safeguard and keep confidential that Private Information.

206. Defendant accepted the special confidence Plaintiffs and Class members placed in it, as evidenced by its assertion that it is "committed to protecting the privacy of [Plaintiffs'] personal information" as included in the Data Breach notification letter.

207. In light of the special relationship between Defendant and Plaintiffs and Class members, whereby Defendant became a guardian of Plaintiffs' and Class members' Private Information, Defendant became a fiduciary by its undertaking and guardianship of the Private Information, to act primarily for the benefit of its customers, including Plaintiffs and Class members for the safeguarding of Plaintiffs' and Class members' Private Information.

208. Defendant has a fiduciary duty to act for the benefit of Plaintiffs and Class members upon matters within the scope of its customer relationships, in particular, to keep secure the Private Information of its customers.

209. Defendant breached its fiduciary duties to Plaintiffs and Class members by failing to protect the integrity of the systems containing Plaintiffs' and Class members' Private Information.

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

211. As a direct and proximate result of Defendant's breaches of its fiduciary duties, Plaintiffs and Class members have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the compromise, publication, and/or theft of their Private Information; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft and/or unauthorized use of their Private Information; (iv) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Cyber-Attack and Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (v) the continued risk to their Private Information, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information in its continued possession; (vi) future costs in terms of time, effort, and money that will be expended as a result of the Cyber-Attack and Data Breach for the remainder of the lives of Plaintiffs and Class Members; and (vii) the diminished value of Defendant's services they received.

212. As a direct and proximate result of Defendant's breaches of its fiduciary duties, Plaintiffs and Class members have suffered and will continue to suffer other forms of injury and/or harm, and other economic and non-economic losses.

COUNT V
DECLARATORY RELIEF
(On Behalf of Plaintiffs and the Nationwide Class or, Alternatively, the State Subclasses)

213. Plaintiffs fully incorporate by reference all of the above paragraphs, as though fully set forth herein.

214. 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 granting further necessary relief. Furthermore, the Court has broad authority to restrain acts, such as here, that are tortious and violate the terms of the federal statutes described in this Complaint.

215. An actual controversy has arisen in the wake of the Data Breach regarding Defendant's present and prospective common law and other duties to reasonably safeguard Plaintiffs' and Class members' PII, and whether Defendant is currently maintaining data security measures adequate to protect Plaintiffs and Class members from future data breaches that compromise their Private Information. Plaintiffs and the Class remain at imminent risk that further compromises of their PII will occur in the future.

216. The Court should also issue prospective injunctive relief requiring Defendant to employ adequate security practices consistent with law and industry standards to protect consumers' PII.

217. Defendant still possesses the PII of Plaintiffs and the Class.

218. To Plaintiffs' knowledge, Defendant has made no announcement that it has changed its data storage or security practices relating to the PII.

219. To Plaintiffs' knowledge, Defendant has made no announcement or notification that it has remedied the vulnerabilities and negligent data security practices that led to the Data Breach.

220. If an injunction is not issued, Plaintiffs and the Class will suffer irreparable injury and lack an adequate legal remedy in the event of another data breach at ReproSource. The risk of another such breach is real, immediate, and substantial.

221. The hardship to Plaintiffs and Class members if an injunction does not issue exceeds the hardship to Defendant if an injunction is issued. Among other things, if another data breach occurs at ReproSource, Plaintiffs and Class members will likely continue to be subjected to fraud, identify theft, and other harms described herein. On the other hand, the cost to Defendant of complying with an injunction by employing reasonable prospective data security measures is relatively minimal, and Defendant has a pre-existing legal obligation to employ such measures.

222. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing another data breach at ReproSource, thus eliminating the additional injuries that would result to Plaintiffs and Class members, along with other consumers whose PII would be further compromised.

223. Pursuant to its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring that ReproSource implement and maintain reasonable security measures, including but not limited to the following:

a. Engaging third-party security auditors/penetration testers, as well as internal security personnel, to conduct testing that includes simulated attacks, penetration tests, and audits on ReproSource's systems on a periodic basis, and ordering ReproSource to promptly correct any problems or issues detected by such third-party security auditors;

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

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

d. purging, deleting, and destroying Private Information not necessary for its provisions of services in a reasonably secure manner;

e. conducting regular database scans and security checks; and

f. 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.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, individually and on behalf of the other members of the Class proposed in this Complaint, respectfully request that the Court enter judgment in favor of Plaintiffs and the Class and against Defendant, as follows:

A. For an Order certifying this action as a class action and appointing Plaintiffs and their counsel to represent the Class;

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

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

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

E. Ordering Defendant to pay for no less than three (3) years of credit monitoring services for Plaintiffs and the Class;

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

G. For an award of punitive damages, as allowable by law;

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

I. Pre- and post-judgment interest on any amounts awarded; and

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

JURY DEMAND

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

Dated: February 21, 2021

Respectfully submitted,

/s/ *David Pastor*
David Pastor (BBO # 391000)
PASTOR LAW OFFICE, LLP
63 Atlantic Avenue, 3rd Floor
Boston, MA 02110
Telephone: 617-742-9700
Facsimile: 617-742-9701
Email: dpastor@pastorlawoffice.com

Nicholas A. Migliaccio
(*pro hac vice* admission to be sought)
Jason S. Rathod, Esquire
(*pro hac vice* admission to be sought)
MIGLIACCIO & RATHOD, LLP
412 H Street, NE, Suite 302
Washington, DC 20002
Phone: 202-470-520
Fax: 202-800-2730
Email: nmigliaccio@classlawdc.com

CERTIFICATE OF SERVICE

I hereby certify that this document filed through the ECF system will be sent electronically to the registered participants as identified on the Notice of Electronic Filing (NEF) and paper copies will be sent to those indicated as non-registered participants on February 21, 2022.

/s/ David Pastor
David Pastor