UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MINNESOTA

DEBORAH PESTER and SHAREN VAN DEN HEUVEL, individually and on behalf of all others similarly situated, Plaintiffs, - against - CONSULTING RADIOLOGISTS, LTD., Defendant.	Case No.: **CLASS ACTION COMPLAINT** Jury Trial Demanded

Plaintiffs Deborah Pester and Sharen Van Den Heuvel ("Plaintiffs"), individually and on behalf of all others similarly situated, by their attorneys, file this class action complaint against Defendant Consulting Radiologists Ltd. ("CRL" or "Defendant"), and in support thereof allege, upon personal knowledge as to their own actions and their counsel's investigation, and upon information and belief as to all other matters, the following:

NATURE OF THE ACTION

1. This class action arises out of a recent cyberattack and data breach ("Data Breach") caused by Defendant's failure to implement reasonable and industry standard data security practices.

2. According to its website, "Consulting Radiologists, Ltd. (CRL) is a physician-owned practice serving patients and providers throughout the Upper Midwest

for more than 90 years."[1] Defendant describes itself as "a leading sub-specialty radiology practice and trusted radiology partner."[2]

3. Plaintiffs bring this Complaint against Defendant for its failure to properly secure and safeguard the sensitive information that it collected and maintained as part of CRL's regular business practices. Such information included, but was not limited to, individuals' names, addresses, dates of birth, Social Security number ("personally identifying information" or "PII") and "Health Insurance information" and "Medical information" ("PHI," and collectively with PII, "Private Information") as defined by the Health Insurance Portability and Accountability Act of 1996 ("HIPAA").[3]

4. Upon information and belief, CRL was entrusted by its patients with sensitive, non-public Private Information, without which CRL could not perform its regular business activities, which includes performing sub-specialty healthcare services and contacting patients' insurance providers. Defendant retains this information for many years and even after retention was necessary for ordinary business purposes or regulatory reasons.

5. By obtaining, collecting, using, and deriving a benefit from the Private Information of Plaintiffs and Class Members, Defendant assumed legal and equitable duties to those individuals to protect and safeguard that information from unauthorized access and intrusion.

---

[1] https://www.consultingradiologists.com/about/ (last visited June 26, 2024).
[2] *Id*.
[3] https://www.consultingradiologists.com/notice-of-data-privacy-event/ (last visited June 26, 2024).

6. According to the letters that CRL sent to Plaintiffs and other impacted Class Members (the "Notice Letter") on or about June 18, 2024, CRL had "detected suspicious activity in its network environment" on February 12, 2024.[4]

7. Plaintiffs and Class Members were notified that CRL investigated this breach, and determined that Private Information was accessed, which may have included their social security number, name, date of birth, address, health insurance information, and medical information.[5]

8. Defendant failed to adequately protect Plaintiffs' and Class Members' Private Information—and failed to even encrypt or redact this highly sensitive information. This unencrypted, unredacted Private Information was compromised due to Defendant's negligent and/or careless acts and omissions and an utter failure to protect the sensitive data it had been entrusted with. Hackers targeted and obtained Plaintiffs' and Class Members' Private Information because of its value in exploiting and stealing the identities of Plaintiffs and Class Members. The present and continuing risk to victims of the Data Breach will remain for their respective lifetimes. By their Complaint, Plaintiffs seek to remedy these harms on behalf of themselves and all similarly situated individuals whose PII and PHI was accessed during the Data Breach.

9. In breaching its duties to properly safeguard Private Information and provide timely, adequate notice of the Data Breach's occurrence, Defendant's conduct amounts to negligence and/or recklessness and violates federal and state statutes.

[4] *See* Notice Letters sent to Plaintiffs, attached hereto as Exhibits A and B; *see also* fn. 3.
[5] *See* fn. 3.

10. Plaintiffs bring this action on behalf of all persons whose Private Information was compromised as a result of Defendant's failure to: (i) adequately protect the Private Information of Plaintiffs and Class Members; (ii) warn Plaintiffs and Class Members of Defendant's inadequate information security practices; and (iii) effectively secure hardware containing protected Private Information using reasonable and effective security procedures free of vulnerabilities and incidents.

11. Defendant disregarded the rights of Plaintiffs and Class Members by intentionally, willfully, recklessly, or negligently failing to implement and maintain adequate and reasonable measures to ensure that the Private Information of Plaintiffs and Class Members was safeguarded, failing to take 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 Private Information of Plaintiffs and Class Members was compromised through disclosure to an unknown and unauthorized third party. Plaintiffs and Class Members have a continuing interest in ensuring that their information is and remains safe, and they should be entitled to injunctive and other equitable relief.

12. Plaintiffs and Class Members have suffered injuries as a result of Defendant's conduct. These injuries include: (i) invasion of privacy; (ii) theft of their Private Information; (iii) lost or diminished value of Private Information; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) experiencing an

increase in spam calls, texts, and/or emails; (viii) statutory damages; (ix) nominal damages; (x) extreme emotional distress; and (xi) the continued and certainly increased risk to their Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up 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.

13. Plaintiffs seek to remedy these harms and prevent any future data compromise on behalf of themselves and all similarly situated persons whose personal data was compromised and stolen as a result of the Data Breach and who remain at risk due to Defendant's inadequate data security practices.

PARTIES

14. Plaintiff Deborah Pester is and has been, at all relevant times, a resident and citizen of Montrose, Minnesota. Plaintiff Pester received a letter from CRL dated June 18, 2024 advising her that her information was compromised in the Data Breach.[6]

15. Plaintiff Sharen Van Den Heuvel is and has been, at all relevant times, a resident and citizen of Cloquet, Minnesota. Plaintiff Van Den Heuvel received a letter from CRL dated June 18, 2024 advising her that her information was compromised in the Data Breach.[7]

[6] *See* Ex. A.
[7] *See* Ex. B.

16. Upon information and belief, Defendant Consulting Radiologists, Ltd. is a domestic business corporation formed under the state laws of Minnesota, with its principal place of business located in Eden Prairie, Minnesota.

JURISDICTION AND VENUE

17. This Court has subject matter jurisdiction pursuant to the Class Action Fairness Act of 2005 ("CAFA"), 28 U.S.C. § 1332(d). The amount in controversy exceeds the sum of $5,000,000 exclusive of interest and costs, there are more than 100 putative class members, and minimal diversity exists because there are putative class members who are citizens of a different state than Defendant. This Court also has supplemental jurisdiction pursuant to 28 U.S.C. § 1367(a) because all claims alleged herein form part of the same case or controversy.

18. This Court has personal jurisdiction over Defendant because it operates and maintains its principal places of business in this District.

19. Venue is proper in this District under 28 U.S.C. § 1391(a) through (d) because Defendant's principal place of business is located in this district and Defendant maintains Class Members' Private Information in this District.

STATEMENT OF FACTS

CRL's Healthcare Business

20. CRL "provide[s] teleradiology-based interpretation services for over 100 healthcare facilities in Minnesota and surrounding areas, outpatient services at convenient

Twin Cities locations, and on-site radiology services for 22 partner hospitals and clinics…."[8]

21. As a prerequisite to the provision of healthcare services, CRL requires its patients to provide sensitive and confidential Private Information, including their names, insurance information, dates of birth, and other personal information.

22. The information held by CRL in its computer systems included the unencrypted Private Information of Plaintiffs and Class Members.

23. CRL's "HIPAA & Privacy Policy" informs patients that, "We learn about you as we care about your health. Some of what we learn becomes part of your health information. We work hard to protect the privacy of your health information and we have rules for our employes on how to manage this information."[9]

24. CRL's "HIPAA & Privacy Policy" further represents that CRL will only allow disclosure of patients' Private Information for purposes of administering healthcare services, communication with insurance, normal organizational operations, billing, public health and safety, research, and to comply with state and federal law when applicable.[10]

25. Upon information and belief, CRL made promises and representations to its clients that the information would be kept safe, confidential, that the privacy of that information would be maintained, and that CRL would delete any sensitive information after it was no longer required to maintain it.

---

[8] *See supra* fn. 1.

[9] *See* https://www.consultingradiologists.com/resources/hipaa-privacy-policy/ (last accessed June 26, 2024).

[10] *Id*.

26. Plaintiffs and Class Members provided their Private Information to CRL with the reasonable expectation and mutual understanding that any custodian of the Private Information would comply with its obligations to keep such information confidential and secure from unauthorized access.

27. Plaintiffs and the Class Members have taken reasonable steps to maintain the confidentiality of their Private Information. Plaintiffs and Class Members relied on the sophistication of CRL to keep their Private Information confidential and securely maintained, to use this information for necessary purposes only, and to make only authorized disclosures of this information. Plaintiffs and Class Members value the confidentiality of their Private Information and demand security to safeguard their Private Information.

28. CRL had a duty to adopt reasonable measures to protect the Private Information of Plaintiffs and Class Members from involuntary disclosure to third parties. CRL has a legal duty to keep Plaintiffs' and Class Members' Private Information safe and confidential.

29. CRL had obligations created by the FTC Act, HIPAA, contract, and industry standards, to keep its patients' and employees' Private Information confidential and to protect it from unauthorized access and disclosure.

30. CRL derived a substantial economic benefit from collecting Plaintiffs' and Class Members' Private Information. Without the required submission of Private Information, CRL could not perform the services it provides, and in turn generate the revenue it does.

31. By obtaining, collecting, using, and deriving a benefit from Plaintiffs' and Class Members' Private Information, CRL 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.

The Data Breach

32. On or about June 18, 2024, CRL began sending Plaintiffs and other victims of the Data Breach the "Notice Letter," informing them, in pertinent part, that:

> On February 12, 2024, CRL detected suspicious activity in its network environment. Upon discovery of this incident, CRL promptly took steps to secure its network and engaged a specialized cybersecurity firm to investigate the nature and scope of the incident. As a result of the investigation, CRL learned that an unauthorized actor accessed certain files and data stored within our network….
> On April 17, 2024, CRL identified persons whose information was included within the data. At this time, we have no evidence any of the information was misused by a third party, but because information related to you was disclosed, we are notifying you out of full transparency…
> The following information was potentially accessed and acquired by a person not authorized to view it: Name, Address, date of birth, Health Insurance information, Medical information.[11]

33. Omitted from the Notice Letter were the dates of CRL's investigation, the details of the root cause of the Data Breach, the vulnerabilities exploited, and the remedial measures undertaken to ensure such a breach does not occur again. To date, these critical facts have not been explained or clarified to Plaintiffs and Class Members, who retain a vested interest in ensuring that their Private Information remains protected.

34. The Notice Letter from CRL also failed to explain why, despite having knowledge of the specific individuals affected by the Data Breach, CRL waited more than

[11] *See* Ex. A and B.

two months to inform Plaintiffs and Class Members that their Private Information had been stolen.

35. CRL's Notice Letter also failed to explain what caused the Data Breach. Nor did CRL explain why its internal investigation took two months to reveal the identities of the affected individuals.

36. This "disclosure" amounts to no real disclosure at all, as it fails to inform, with any degree of specificity, Plaintiffs and Class Members of the Data Breach's critical facts. Without these details, the ability to mitigate the harms resulting from the Data Breach is severely diminished.

37. CRL did not use reasonable security procedures and practices appropriate to the nature of the sensitive information it was maintaining for Plaintiffs and Class Members, causing the exposure of Private Information, such as encrypting the information or deleting it when it is no longer needed.

38. The attacker accessed and acquired files in CRL's computer systems containing unencrypted Private Information of Plaintiffs and Class Members, including their names, dates of birth, PHI, and other sensitive information. Plaintiffs' and Class Members' Private Information was accessed and stolen in the Data Breach.

39. Plaintiffs further believe that their Private Information and that of Class Members was or will be sold on the dark web, as that is the modus operandi of cybercriminals that commit cyber-attacks of this type.

Data Breaches Are Preventable

40. As explained by the Federal Bureau of Investigation ("FBI"), "[p]revention is the most effective defense against ransomware and it is critical to take precautions for protection."[12]

41. To prevent and detect cyber-attacks and/or ransomware attacks 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.

- 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

[12] *See* How to Protect Your Networks from RANSOMWARE, at 3, available at https://www.fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf/view

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 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.[13]

42. To prevent and detect cyber-attacks or ransomware attacks, Defendant could and should have implemented, as recommended by the Microsoft Threat Protection Intelligence Team, the following measures:

Secure internet-facing assets

- Apply latest security updates
- Use threat and vulnerability management
- Perform regular audit; remove privileged credentials;

[13] *Id.* at 3-4.

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
- Analyze logon events
- Turn on attack surface reduction rules and [Antimalware Scan Interface] for Office [Visual Basic for Applications].[14]

43. Given that Defendant was storing sensitive Private Information, Defendant could and should have implemented the above measures to prevent and detect cyberattacks.

44. The occurrence of the Data Breach indicates that Defendant failed to adequately implement one or more of the above measures to prevent cyberattacks, resulting

[14] *See* Human-operated ransomware attacks: A preventable disaster (Mar. 5, 2020), *available at:* https://microsoft.com/security/blog/2020/03/05/human-operated-ransomware-attacks-a-preventable-disaster/.

in the Data Breach and the exposure of the Private Information of a large number of people, including that of Plaintiffs and Class Members.

Defendant Acquires, Collects, and Stores Plaintiffs' and Class Members' Private Information

45. As a condition to obtain medical services from CRL, CRL requires its patients to give their sensitive and confidential Private Information to them, with the understanding that only limited, trusted third parties, may come into possession of this Private Information.

46. Defendant retains and stores this information and derives a substantial economic benefit from the Private Information that it collects. But for the collection of Plaintiffs' and Class Members' Private Information, Defendant would be unable to perform its services.

47. By obtaining, collecting, and storing the Private Information of Plaintiffs and Class Members, Defendant assumed legal and equitable duties and knew or should have known that it was responsible for protecting the Private Information from disclosure.

48. Plaintiffs and Class Members have taken reasonable steps to maintain the confidentiality of their Private Information and relied on Defendant to keep their Private Information confidential and maintained securely, to use this information for business purposes only, and to make only authorized disclosures of this information.

49. Defendant could have prevented this Data Breach by properly securing and encrypting the files and file servers containing the Private Information of Plaintiffs and Class Members.

50. Upon information and belief, Defendant made promises to the owners of the Private Information, by and through its relationships with its clients, to maintain and protect their Private Information, demonstrating an understanding of the importance of securing Private Information.

51. Defendant's negligence in safeguarding the Private Information of Plaintiffs and Class Members is exacerbated by the repeated warnings and alerts directed to protecting and securing sensitive data.

Defendant Knew, or Should Have Known, of the Risk Because Entities in Healthcare in Possession of Private Information Are Particularly Susceptible to Cyber Attacks

52. Data thieves regularly target companies in the health care sector like Defendant due to the highly sensitive information that they keep. Defendant knew and understood that unprotected Private Information is valuable and highly sought after by criminal parties who seek to illegally monetize that Private Information through unauthorized access.

53. Defendant's data security obligations were particularly important given the substantial increase in cyber-attacks and/or data breaches targeting healthcare entities that collect and store Private Information and other sensitive information, like Defendant, preceding the date of the breach.

54. In the third quarter of the 2023 fiscal year alone, 7,333 organizations experienced data breaches, resulting in 66,658,764 individuals' personal information being compromised.[15]

55. In light of recent high profile cybersecurity incidents at other healthcare partner and provider companies, including American Medical Collection Agency (25 million patients, March 2019), University of Washington Medicine (974,000 patients, December 2018), Florida Orthopedic Institute (640,000 patients, July 2020), Wolverine Solutions Group (600,000 patients, September 2018), Oregon Department of Human Services (645,000 patients, March 2019), Elite Emergency Physicians (550,000 patients, June 2020), Magellan Health (365,000 patients, April 2020), and BJC Health System (286,876 patients, March 2020), Defendant knew or should have known that its electronic records would be targeted by cybercriminals.

56. Indeed, cyber-attacks, such as the one experienced by Defendant, have become so notorious that the FBI and U.S. Secret Service have issued a warning to potential targets, so they are aware of, and prepared for, a potential attack. As one report explained, smaller entities that store Private Information are "attractive to ransomware criminals…because they often have lesser IT defenses and a high incentive to regain access to their data quickly."[16]

[15] *See* https://www.idtheftcenter.org/publication/q3-data-breach-2023-analysis/
[16] https://www.law360.com/articles/1220974/ (last accessed Apr. 30, 2024).

57. Additionally, as companies became more dependent on computer systems to run their business,[17] *e.g.*, working remotely as a result of the COVID-19 pandemic, and the Internet of Things ("IoT"), the danger posed by cybercriminals is magnified, thereby highlighting the need for adequate administrative, physical, and technical safeguards.[18]

58. Despite the prevalence of public announcements of data breach and data security compromises, Defendant failed to take appropriate steps to protect the Private Information of Plaintiffs and Class Members from being compromised.

59. As a custodian of Private Information, Defendant knew, or should have known, the importance of safeguarding the Private Information entrusted to it by Plaintiffs and Class Members, and of the foreseeable consequences if its data security systems were breached, including the significant costs imposed on Plaintiffs and Class Members as a result of a breach.

60. At all relevant times, Defendant knew, or reasonably should have known, of the importance of safeguarding the Private Information of Plaintiffs and Class Members and of the foreseeable consequences that would occur if Defendant's data security systems were breached, including, specifically, the significant costs that would be imposed on Plaintiffs and Class Members as a result of a breach.

[17] https://www.federalreserve.gov/econres/notes/feds-notes/implications-of-cyber-risk-for-financial-stability-20220512.html (last accessed Apr. 30, 2024).
[18] https://www.picussecurity.com/key-threats-and-cyber-risks-facing-financial-services-and-banking-firms-in-2022 (last accessed Apr. 30, 2024).

61. Defendant was, or should have been, fully aware of the unique type and the significant volume of data on its server(s), and, thus, the significant number of individuals who would be harmed by the exposure of the unencrypted data.

62. The injuries to Plaintiffs and Class Members were directly and proximately caused by Defendant's failure to implement or maintain adequate data security measures for the Private Information of Plaintiffs and Class Members.

63. The ramifications of Defendant's failure to keep secure the Private Information of Plaintiffs and Class Members are long lasting and severe. Once Private Information is stolen—particularly PHI—fraudulent use of that information and damage to victims may continue for years.

64. As a company in possession of individuals' Private Information, including PHI, Defendant knew, or should have known, the importance of safeguarding the Private Information entrusted to it by Plaintiffs and Class Members and of the foreseeable consequences if its data security systems were breached. This includes the significant costs imposed on Plaintiffs and Class Members as a result of a breach. Nevertheless, Defendant failed to take adequate cybersecurity measures to prevent the Data Breach.

Value of Private Information

65. The Federal Trade Commission ("FTC") defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority."[19] The FTC describes "identifying information" as "any name or number that

[19] 17 C.F.R. § 248.201 (2013).

may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number."[20]

66. The PII of individuals remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials.[21]

67. For example, Private Information can be sold at a price ranging from $40 to $200.[22] Criminals can also purchase access to entire company data breaches from $900 to $4,500.[23]

68. Theft of PHI is also gravely serious: "[a] thief may use your name or health insurance numbers to see a doctor, get prescription drugs, file claims with your insurance provider, or get other care. If the thief's health information is mixed with yours, your treatment, insurance and payment records, and credit report may be affected." [24]

---

[20] *Id.*

[21] *Your personal data is for sale on the dark web. Here's how much it costs,* Digital Trends, Oct. 16, 2019, *available at*: https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/

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

[23] *In the Dark*, VPNOverview, 2019, *available at*: https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/

[24] https://efraudprevention.net/home/education/?a=187#:%7E:text=A%20thief%20may%20use%20your,credit%20report%20may%20be%20affected

69. The greater efficiency of electronic health records brings the risk of privacy breaches. These electronic health records contain a lot of sensitive information (e.g., patient data, patient diagnosis, lab results, medications, prescriptions, treatment plans, etc.) that is valuable to cybercriminals. One patient's complete record can be sold for hundreds of dollars on the dark web. As such, Private Information is a valuable commodity for which a "cyber black market" exists where criminals openly post stolen payment card numbers, Social Security numbers, and other personal information on several underground internet websites. Unsurprisingly, the healthcare industry is at high risk and is acutely affected by cyberattacks, like the Data Breach here.

70. Between 2005 and 2019, at least 249 million people were affected by healthcare data breaches.[25] Indeed, during 2019 alone, over 41 million healthcare records were exposed, stolen, or unlawfully disclosed in 505 data breaches.[26] In short, these sorts of data breaches are increasingly common, especially among healthcare systems, which account for 30.03 percent of overall health data breaches, according to cybersecurity firm Tenable.[27]

71. "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,

[25] https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7349636/#B5-healthcare-08-00133/
[26] https://www.hipaajournal.com/december-2019-healthcare-data-breach-report/
[27] https://www.tenabhle.com/blog/healthcare-security-ransomware-plays-a-prominent-role-incovid-19-era-breaches/

they frequently discover erroneous information has been added to their personal medical files due to the thief's activities."[28]

72. A study by Experian found that the average cost of medical identity theft is "about $20,000" per incident and that most victims of medical identity theft were forced to pay out-of-pocket costs for healthcare they did not receive to restore coverage.[29] Almost half of medical identity theft victims lose their healthcare coverage as a result of the incident, while nearly one-third of medical identity theft victims saw their insurance premiums rise, and 40 percent were never able to resolve their identity theft at all.[30]

73. Based on the foregoing, the information compromised in the Data Breach is significantly more valuable than the loss of, for example, credit card information in a retailer data breach because, there, victims can cancel or close credit and debit card accounts. The information compromised in this Data Breach is impossible to "close" and difficult, if not impossible to change – names, dates of birth, and PHI.

74. This data demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "Compared to credit card information, personally identifiable information . . . [is] worth more than 10x on the black market."[31]

---

[28] Michael Ollove, "The Rise of Medical Identity Theft in Healthcare," Kaiser Health News, Feb. 7, 2014, https://khn.org/news/rise-of-indentity-theft/

[29] *See* Elinor Mills, "Study: Medical Identity Theft is Costly for Victims," CNET (Mar, 3, 2010), https://www.cnet.com/news/study-medical-identity-theft-is-costly-for-victims/

[30] *Id.*; *see also* Healthcare Data Breach: What to Know About them and What to Do After One, EXPERIAN, https://www.experian.com/blogs/ask-experian/healthcare-data-breach-what-toknow-about-them-and-what-to-do-after-one/

[31] Tim Greene, Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit

75. Among other forms of fraud, identity thieves may obtain driver's licenses, government benefits, medical services, and housing or even give false information to police.

76. The fraudulent activity resulting from the Data Breach may not come to light for years. There may be a time lag between when harm occurs versus when it is discovered, and also between when Private Information is stolen and when it is used. According to the U.S. Government Accountability Office ("GAO"), which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[32]

77. Plaintiffs and Class Members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. The Class is incurring and will continue to incur such damages in addition to any fraudulent use of their Private Information.

Card Numbers, IT World, (Feb. 6, 2015), available at: https://www.networkworld.com/article/2880366/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html

[32] Report to Congressional Requesters, GAO, at 29 (June 2007), available at: https://www.gao.gov/assets/gao-07-737.pdf

Defendant Fails to Comply with FTC Guidelines

78. The FTC has promulgated numerous guides for businesses which highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.

79. In 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which established cyber-security guidelines for businesses. These guidelines note that businesses should protect the personal patient 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.[33]

80. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.[34]

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

---

[33] *Protecting Personal Information: A Guide for Business*, Federal Trade Commission (2016). Available at https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf

[34] *Id.*

82. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect patient data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential patient data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTC Act"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

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

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

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

86. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to Private Information it stored or to comply with applicable industry standards constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

87. Upon information and belief, Defendant was at all times fully aware of its obligation to protect the Private Information it came into possession of. Defendant was also aware of the significant repercussions that would result from its failure to do so. Accordingly, Defendant's conduct was particularly unreasonable given the nature and amount of Private Information it obtained and stored and the foreseeable consequences of the immense damages that would result to Plaintiffs and the Class.

Defendant Fails to Comply with HIPAA Guidelines

88. Defendant is a health care provider that transmits health information in electronic form under HIPAA (45 C.F.R. § 160.102) and is required to comply with the HIPAA Privacy Rule and Security Rule, 45 C.F.R. Part 160 and Part 164, Subparts A and E ("Standards for Privacy of Individually Identifiable Health Information"), and Security Rule ("Security Standards for the Protection of Electronic Protected Health Information"), 45 C.F.R. Part 160 and Part 164, Subparts A and C.

89. Defendant is subject to the rules and regulations for safeguarding electronic forms of medical information pursuant to the Health Information Technology Act ("HITECH").[35] *See* 42 U.S.C. §17921, 45 C.F.R. § 160.103.

90. HIPAA's Privacy Rule or *Standards for Privacy of Individually Identifiable Health Information* establishes national standards for the protection of health information.

[35] HIPAA and HITECH work in tandem to provide guidelines and rules for maintaining protected health information. HITECH references and incorporates HIPAA.

91. HIPAA's Privacy Rule or *Security Standards for the Protection of Electronic Protected Health Information* establishes a national set of security standards for protecting health information that is kept or transferred in electronic form.

92. HIPAA requires "compl[iance] with the applicable standards, implementation specifications, and requirements" of HIPAA "with respect to electronic protected health information." 45 C.F.R. § 164.302.

93. "Electronic protected health information" is "individually identifiable health information … that is (i) transmitted by electronic media; maintained in electronic media." 45 C.F.R. § 160.103.

94. HIPAA's Security Rule requires Defendant to do the following:

a. Ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity or business associate creates, receives, maintains, or transmits;
b. Protect against any reasonably anticipated threats or hazards to the security or integrity of such information;
c. Protect against any reasonably anticipated uses or disclosures of such information that are not permitted; and
d. Ensure compliance by their respective workforce.

95. HIPAA also requires Defendant to "review and modify the security measures implemented … as needed to continue provision of reasonable and appropriate protection of electronic protected health information." 45 C.F.R. § 164.306(e). Additionally, Defendant is required under HIPAA to "[i]mplement 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." 45 C.F.R. § 164.312(a)(1).

96. HIPAA and HITECH also obligated Defendant to implement policies and procedures to prevent, detect, contain, and correct security violations, and to protect against uses or disclosures of electronic protected health information that are reasonably anticipated but not permitted by the privacy rules. *See* 45 C.F.R. § 164.306(a)(1) and § 164.306(a)(3); *see also* 42 U.S.C. § 17902.

97. The HIPAA Breach Notification Rule, 45 C.F.R. §§ 164.400-414, also requires Defendant to provide notice of the Data Breach to each affected individual "without unreasonable delay and in no case later than 60 days following discovery of the breach."[36]

98. HIPAA also requires the Office of Civil Rights ("OCR"), within the Department of Health and Human Services ("HHS"), to issue annual guidance documents on the provisions in the HIPAA Security Rule. *See* 45 C.F.R. §§ 164.302-164.318. For example, "HHS has developed guidance and tools to assist HIPAA covered entities in identifying and implementing the most cost effective and appropriate administrative, physical, and technical safeguards to protect the confidentiality, integrity, and availability of e-PHI and comply with the risk analysis requirements of the Security Rule." US Department of Health & Human Services, Security Rule Guidance Material.[37] The list of

[36] Breach Notification Rule, U.S. Dep't of Health & Human Services, https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html.
[37] http://www.hhs.gov/hipaa/for-professionals/security/guidance/index.html.

resources includes a link to guidelines set by the National Institute of Standards and Technology (NIST), which OCR says "represent the industry standard for good business practices with respect to standards for securing e-PHI." US Department of Health & Human Services, Guidance on Risk Analysis.[38]

Defendant Fails to Comply with Industry Standards

99. As noted above, experts studying cyber security routinely identify healthcare entities in possession of Private Information as being particularly vulnerable to cyberattacks because of the value of the Private Information which they collect and maintain.

100. Several best practices have been identified that, at a minimum, should be implemented by healthcare entities like Defendant in possession of Private Information, including but not limited to: educating all employees; strong passwords; multi-layer security, including firewalls, anti-virus, and anti-malware software; encryption, making data unreadable without a key; multi-factor authentication; backup data and limiting which employees can access sensitive data. Defendant failed to follow these industry best practices, including a failure to implement multi-factor authentication.

101. Other best cybersecurity practices that are standard in the healthcare industry include installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches and routers; monitoring and protection of

[38] https://www.hhs.gov/hipaa/for-professionals/security/guidance/guidance-risk-analysis/index.html

physical security systems; protection against any possible communication system; and training staff regarding critical points. Defendant failed to follow these cybersecurity best practices, including failure to train staff.

102. Defendant failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

103. These foregoing frameworks are existing and applicable industry standards in the healthcare industry, and upon information and belief, Defendant failed to comply with at least one—or all—of these accepted standards, thereby opening the door to the threat actor and causing the Data Breach.

COMMON INJURIES AND DAMAGES

104. As a result of Defendant's ineffective and inadequate data security practices, the Data Breach, and the foreseeable consequences of Private Information ending up in the possession of criminals, the risk of identity theft to the Plaintiffs and Class Members has materialized and is imminent, and Plaintiffs and Class Members have all sustained actual injuries and damages, including: (i) invasion of privacy; (ii) theft of their Private Information; (iii) lost or diminished value of Private Information; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with

attempting to mitigate the actual consequences of the Data Breach; (vii) statutory damages; (viii) nominal damages; and (ix) the continued and certainly increased risk to their Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up 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.

The Data Breach Increases Victims' Risk of Identity Theft

105. The unencrypted Private Information of Plaintiffs and Class Members will end up for sale on the dark web as that is the *modus operandi* of hackers.

106. Unencrypted Private Information may also fall into the hands of companies that will use the detailed Private Information for targeted marketing without the approval of Plaintiffs and Class Members. Simply, unauthorized individuals can easily access the Private Information of Plaintiffs and Class Members.

107. The link between a data breach and the risk of identity theft is simple and well established. Criminals acquire and steal Private Information to monetize the information. Criminals monetize the data by selling the stolen information on the black market to other criminals who then utilize the information to commit a variety of identity theft related crimes discussed below.

108. Plaintiffs' and Class Members' Private Information is of great value to hackers and cyber criminals, and the data stolen in the Data Breach has been used and will continue to be used in a variety of sordid ways for criminals to exploit Plaintiffs and Class Members and to profit off their misfortune.

109. One such example of criminals piecing together bits and pieces of compromised PII for profit is the development of "Fullz" packages.[39]

110. With "Fullz" packages, cyber-criminals can cross-reference two sources of Private Information to marry unregulated data available elsewhere to criminally stolen data with an astonishingly complete scope and degree of accuracy in order to assemble complete dossiers on individuals.

111. The development of "Fullz" packages means here that the stolen Private Information from the Data Breach can easily be used to link and identify it to Plaintiffs' and Class Members' phone numbers, email addresses, and other unregulated sources and identifiers. In other words, even if certain information such as emails, phone numbers, or credit card numbers may not be included in the Private Information that was exfiltrated in the Data Breach, criminals may still easily create a Fullz package and sell it at a higher

[39] "Fullz" is fraudster speak for data that includes the information of the victim, including, but not limited to, the name, address, credit card information, social security number, date of birth, and more. As a rule of thumb, the more information you have on a victim, the more money that can be made off of those credentials. Fullz are usually pricier than standard credit card credentials, commanding up to $100 per record (or more) on the dark web. Fullz can be cashed out (turning credentials into money) in various ways, including performing bank transactions over the phone with the required authentication details in-hand. Even "dead Fullz," which are Fullz credentials associated with credit cards that are no longer valid, can still be used for numerous purposes, including tax refund scams, ordering credit cards on behalf of the victim, or opening a "mule account" (an account that will accept a fraudulent money transfer from a compromised account) without the victim's knowledge. See, e.g., Brian Krebs, Medical Records for Sale in Underground Stolen From Texas Life Insurance Firm, Krebs on Security (Sep. 18, 2014), https://krebsonsecuritv.eom/2014/09/medical-records-for-sale-in-underground-stolen-from-texas-life-insurance-](https://krebsonsecuritv.eom/2014/09/medical-records-for-sale-in-underground-stolen-from-texas-life-insurance-finn/.

price to unscrupulous operators and criminals (such as illegal and scam telemarketers) over and over.

112. The existence and prevalence of "Fullz" packages means that the Private Information stolen from the data breach can easily be linked to the unregulated data (like phone numbers and emails) of Plaintiffs and the other Class Members.

113. Thus, even if certain information was not stolen in the data breach, criminals can still easily create a comprehensive "Fullz" package.

114. Then, this comprehensive dossier can be sold—and then resold in perpetuity—to crooked operators and other criminals (like illegal and scam telemarketers).

Loss of Time to Mitigate the Risk of Identity Theft and Fraud

115. As a result of the recognized risk of identity theft, when a Data Breach occurs, and an individual is notified by a company that their Private Information was compromised, as in this Data Breach, the reasonable person is expected to take steps and spend time to address the dangerous situation, learn about the breach, and otherwise mitigate the risk of becoming a victim of identity theft of fraud. Failure to spend time taking steps to review accounts or credit reports could expose the individual to greater financial harm – yet, the resource and asset of time has been lost.

116. Thus, due to the actual and imminent risk of identity theft, CRL provided, in its Notice Letter, steps on how to obtain credit reports and freeze credit accounts.[40] Moreover, CRL reminded victims that they, and not CRL, are responsible for mitigating

[40] *See* Ex. A

the effects of the Data Breach by instructing Plaintiffs and Class Members to "remain vigilant and monitor [their] accounts for suspicious or unusual activity."[41] CRL did not offer victims any credit monitoring services.

117. Plaintiffs and Class Members have spent, and will spend additional time in the future, on a variety of prudent actions, such as researching and verifying the legitimacy of the Data Breach, replacing credit cards, and monitoring their financial accounts for any indication of fraudulent activity, which may take years to detect.

118. Plaintiffs' mitigation efforts are consistent with the U.S. Government Accountability Office that released a report in 2007 regarding data breaches ("GAO Report") in which it noted that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."[42]

119. Plaintiffs' mitigation efforts are also consistent with the steps that FTC recommends that data breach victims take several steps to protect their personal and financial information after a data breach, including: contacting one of the credit bureaus to place a fraud alert (consider an extended fraud alert that lasts for seven years if someone steals their identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.[43]

---

[41] *Id.*

[42] *See* United States Government Accountability Office, GAO-07-737, Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown (June 2007), https://www.gao.gov/new.items/d07737.pdf.

[43] *See* Federal Trade Commission, Identity Theft.gov,

120. And for those Class Members who experience actual identity theft and fraud, GAO Report notes that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."[44]

Diminution of Value of PII and PHI

121. PII and PHI are valuable property rights.[45] Their value is axiomatic, considering the value of Big Data in corporate America and the consequences of cyber thefts include heavy prison sentences. Even this obvious risk to reward analysis illustrates beyond doubt that Private Information has considerable market value.

122. Sensitive PII can sell for as much as $363 per record according to the Infosec Institute.[46]

123. An active and robust legitimate marketplace for PII also exists. In 2019, the data brokering industry was worth roughly $200 billion.[47]

124. In fact, the data marketplace is so sophisticated that consumers can actually sell their non-public information directly to a data broker who in turn aggregates the information and provides it to marketers or app developers.[48] Consumers who agree to

---

https://www.identitytheft.gov/Steps

[44] *See* GAO Report, p. 2

[45] *See, e.g.,* John T. Soma, et al, Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("PII") Equals the "Value" of Financial Assets, 15 Rich. J.L. & Tech. 11, at *3-4 (2009) ("Private Information, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets.") (citations omitted).

[46] *See* Ashiq Ja, Hackers Selling Healthcare Data in the Black Market, InfoSec (July 27, 2015), https://resources.infosecinstitute.com/topic/hackers-selling-healthcare-data-in-the-black-market/

[47] https://www.latimes.com/business/story/2019-11-05/column-data-brokers

[48] https://datacoup.com/

provide their web browsing history to the Nielsen Corporation can receive up to $50.00 a year.[49]

125. According to account monitoring company LogDog, medical data sells for $50 and up on the Dark Web.[50]

126. As a result of the Data Breach, Plaintiffs' and Class Members' Private Information, which has an inherent market value in both legitimate and dark markets, has been damaged and diminished by its compromise and unauthorized release. However, this transfer of value occurred without any consideration paid to Plaintiffs or Class Members for their property, resulting in an economic loss. Moreover, the Private Information is now readily available, and the rarity of the data has been lost, thereby causing additional loss of value.

127. At all relevant times, Defendant knew, or reasonably should have known, of the importance of safeguarding the Private Information of Plaintiffs and Class Members, and of the foreseeable consequences that would occur if Defendant's data security systems were breached, including, specifically, the significant costs that would be imposed on Plaintiffs and Class Members as a result of a breach.

128. The fraudulent activity resulting from the Data Breach may not come to light for years.

[49] https://digi.me/what-is-digime/

[50] Lisa Vaas, Ransomware Attacks Paralyze, and Sometimes Crush, Hospitals, Naked Security (Oct. 3, 2019), https://nakedsecurity.sophos.com/2019/10/03/ransomware-attacks-paralyze-and-sometimes-crush-hospitals/#content

129. Plaintiffs and Class Members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. The Class is incurring and will continue to incur such damages in addition to any fraudulent use of their Private Information.

130. Defendant was, or should have been, fully aware of the unique type and the significant volume of data on Defendant's network, amounting to a large number of individuals' detailed personal information and, thus, the significant number of individuals who would be harmed by the exposure of the unencrypted data.

131. The injuries to Plaintiffs and Class Members were directly and proximately caused by Defendant's failure to implement or maintain adequate data security measures for the Private Information of Plaintiffs and Class Members.

Future Cost of Credit and Identity Theft Monitoring Is Reasonable and Necessary

132. Given the type of targeted attack in this case, sophisticated criminal activity, and the type of Private Information involved, there is a strong probability that entire batches of stolen information have been placed, or will be placed, on the black market/dark web for sale and purchase by criminals intending to utilize the Private Information for identity theft crimes–e.g., opening bank accounts in the victims' names to make purchases or to launder money; file false tax returns; take out loans or lines of credit; or file false unemployment claims.

133. Such fraud may go undetected until debt collection calls commence months, or even years, later. An individual may not know that his or her Private Information was

used to file for unemployment benefits until law enforcement notifies the individual's employer of the suspected fraud. Fraudulent tax returns are typically discovered only when an individual's authentic tax return is rejected.

134. Consequently, Plaintiffs and Class Members are at an increased risk of fraud and identity theft for many years into the future.

135. The retail cost of credit monitoring and identity theft monitoring can cost around $200 a year per Class Member. This is a reasonable and necessary cost to monitor to protect Class Members from the risk of identity theft that arose from Defendant's Data Breach.

Loss of Benefit of the Bargain

136. Furthermore, Defendant's poor data security deprived Plaintiffs and Class Members of the benefit of their bargain. When agreeing to obtain medical services from CRL under certain terms, Plaintiffs and other reasonable patients understood and expected that Defendant would properly safeguard and protect their Private Information, when in fact, Defendant did not provide the expected data security. Accordingly, Plaintiffs and Class Members received medical services of a lesser value than what they reasonably expected to receive under the bargains they struck with Defendant.

PLAINTIFFS' EXPERIENCE

Plaintiff Pester

137. Plaintiff Pester has been treated in CRL health care facilities in Minnesota for over 25 years.

138. As a condition of obtaining medical services from these facilities, Plaintiff was required to provide her Private Information, including her name, social security number, health insurance information, date of birth, and other sensitive information.

139. Upon information and belief, at the time of the Data Breach, Defendant had retained Plaintiffs' Private Information on its system.

140. Plaintiff is very careful about sharing her sensitive Private Information. Plaintiff stores any documents containing her Private Information in a safe and secure location. She has never knowingly transmitted unencrypted sensitive Private Information over the internet or any other unsecured source. Had Plaintiff known that Defendant would fail to implement reasonable and adequate data security safeguards, she would not have permitted her Private Information to be shared.

141. Plaintiff received the Notice Letter, by U.S. mail shortly after June 18, 2024, informing her that her Private Information was improperly accessed and obtained by unauthorized third parties during the Data Breach.

142. As a result of the Data Breach and at the direction of the Notice Letter, which instructed her to "remain vigilant and monitor [her] accounts for suspicious or unusual activity,"[51] Plaintiff made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to: researching and verifying the legitimacy of the Data Breach, and monitoring her financial accounts for any indication of fraudulent activity, which may take years to detect. Plaintiff has spent significant time remedying the breach—valuable

[51] *See* Ex. A.

time Plaintiff otherwise would have spent on other activities, including but not limited to work and/or recreation. This time has been lost forever and cannot be recaptured.

143. Plaintiff suffered actual injury from having her Private Information compromised as a result of the Data Breach including, but not limited to: (i) unauthorized charges to her credit card; (ii) invasion of privacy; (iii) theft of her Private Information; (iv) lost or diminished value of Private Information; (v) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vi) loss of benefit of the bargain; (vii) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (viii) statutory damages; (ix) nominal damages; (x) severe anxiety and extreme emotional distress; and (xi) the continued and certainly increased risk to her Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up 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.

144. Plaintiff further suffered actual injury in the form of experiencing an increase in spam calls, texts, and/or emails, which, upon information and belief, was caused by the Data Breach.

145. The Data Breach has caused Plaintiff to suffer fear, anxiety, and stress, which has been compounded by the fact that Defendant has still not fully informed her of key details about the Data Breach's occurrence.

146. As a result of the Data Breach, Plaintiff anticipates spending considerable time on an ongoing basis to try to mitigate and address harms caused by the Data Breach.

147. As a result of the Data Breach, Plaintiff is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

148. Plaintiff has a continuing interest in ensuring that her Private Information, which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future breaches.

Plaintiff Van Den Heuvel

149. Plaintiff Van Den Heuvel has been treated in CRL health care facilities in Minnesota for over 25 years.

150. As a condition of obtaining medical services from these facilities, Plaintiff was required to provide her Private Information, including her name, social security number, health insurance information, date of birth, and other sensitive information.

151. Upon information and belief, at the time of the Data Breach, Defendant had retained Plaintiffs' Private Information on its system.

152. Plaintiff is very careful about sharing her sensitive Private Information. Plaintiff stores any documents containing her Private Information in a safe and secure location. She has never knowingly transmitted unencrypted sensitive Private Information over the internet or any other unsecured source. Had Plaintiff known that Defendant would fail to implement reasonable and adequate data security safeguards, she would not have permitted her Private Information to be shared.

153. Plaintiff received the Notice Letter, by U.S. mail shortly after June 18, 2024, informing her that her Private Information was improperly accessed and obtained by unauthorized third parties during the Data Breach.

154. As a result of the Data Breach and at the direction of the Notice Letter, which instructed her to "remain vigilant and monitor [her] accounts for suspicious or unusual activity,"[52] Plaintiff made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to: researching and verifying the legitimacy of the Data Breach, and monitoring her financial accounts for any indication of fraudulent activity, which may take years to detect. Plaintiff has spent significant time remedying the breach—valuable time Plaintiff otherwise would have spent on other activities, including but not limited to work and/or recreation. This time has been lost forever and cannot be recaptured.

155. Plaintiff suffered actual injury from having her Private Information compromised as a result of the Data Breach including, but not limited to: (i) unauthorized charges to their credit card; (ii) invasion of privacy; (iii) theft of their Private Information; (iv) lost or diminished value of Private Information; (v) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vi) loss of benefit of the bargain; (vii) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (viii) statutory damages; (ix) nominal damages; (x) severe anxiety and extreme emotional distress; and (xi) the continued and certainly increased risk to their Private Information, which: (a) remains unencrypted and

[52] See Ex. B.

available for unauthorized third parties to access and abuse; and (b) remains backed up 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.

156. Plaintiff further suffered actual injury in the form of experiencing an increase in spam calls, texts, and/or emails, which, upon information and belief, was caused by the Data Breach.

157. The Data Breach has caused Plaintiff to suffer fear, anxiety, and stress, which has been compounded by the fact that Defendant has still not fully informed her of key details about the Data Breach's occurrence.

158. As a result of the Data Breach, Plaintiff anticipates spending considerable time on an ongoing basis to try to mitigate and address harms caused by the Data Breach.

159. As a result of the Data Breach, Plaintiff is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

160. Plaintiff has a continuing interest in ensuring that her Private Information, which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future breaches.

CLASS ACTION ALLEGATIONS

161. Pursuant to Federal Rule of Civil Procedure 23, Plaintiffs propose the following Class definition, subject to amendment as appropriate:

> All persons whose Private Information was maintained by Defendant that was compromised in the Data Breach announced by CRL on or about June 18, 2024 (the "Class").

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

163. Plaintiffs hereby reserve the right to amend or modify the Class definition with greater specificity or division after having had an opportunity to conduct discovery.

164. Numerosity. The Members of the Class are so numerous that joinder of all of them is impracticable. The exact number of Class Members is unknown to Plaintiffs at this time, but is believed to be in excess of 510,000.[53]

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

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

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

[53] https://www.maine.gov/agviewer/content/ag/985235c7-cb95-4be2-8792-a1252b4f8318/e3a918a6-607e-4012-8b0b-f09f5c7ea512.html (last accessed June 26, 2024).

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

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

e. Whether Defendant owed a duty to Class Members to safeguard their Private Information;

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

g. Whether computer hackers obtained Class Members' Private Information in the Data Breach;

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

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

j. Whether Defendant's conduct was negligent;

k. Whether Defendant breached implied contracts for adequate data security with Plaintiffs and Class Members;

l. Whether Defendant was unjustly enriched by retention of the monetary benefits conferred on it by Plaintiffs and Class Members;

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

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

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

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

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

169. Superiority. A class action is superior to other available methods for the fair and efficient adjudication of the controversy. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a class action, most Class Members would likely find that the cost of litigating their individual claims is prohibitively high and would therefore have no effective remedy. The prosecution of separate actions by individual Class Members would create a risk of inconsistent or varying adjudications with respect to individual Class Members, which would establish incompatible standards of conduct for Defendant. In contrast, the conduct of this action as

a class action presents far fewer management difficulties, conserves judicial resources and the parties' resources, and protects the rights of each Class Member.

170. Defendant has acted on grounds that apply generally to the Class as a whole, so that class certification, injunctive relief, and corresponding declaratory relief are appropriate on a class-wide basis.

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

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

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

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

d. Whether Defendant failed to take commercially reasonable steps to safeguard consumer Private Information; and

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

172. Finally, all Members of the proposed Class are readily ascertainable. Defendant has access to Class Members' names and addresses affected by the Data Breach.

Class Members have already been preliminarily identified and sent the Notice Letter by CRL.

FIRST CAUSE OF ACTION
NEGLIGENCE
(On Behalf of Plaintiffs and the Class)

173. Plaintiffs repeat, re-allege, and incorporate by reference, all other paragraphs of this complaint.

174. Defendant gathered and stored the Private Information of Plaintiffs and Class Members as part of their business of soliciting its services, which solicitations and services affect commerce.

175. Plaintiffs and Class Members entrusted Defendant with their Private Information with the understanding that Defendant would safeguard their information.

176. Defendant had full knowledge of the sensitivity of the Private Information and the types of harm that Plaintiffs and Class Members could and would suffer if the Private Information were wrongfully disclosed.

177. By assuming the responsibility to collect and store this data, and in fact doing so, and sharing it and using it for commercial gain, Defendant had a duty of care to use reasonable means to secure and safeguard its computer property—and Class Members' Private Information held within it—to prevent disclosure of the information, and to safeguard the information from theft. Defendant's duty included a responsibility to implement processes by which it could detect a breach of its security systems in a reasonably expeditious period of time and to give prompt notice to those affected in the case of a data breach.

178. Defendant had a duty to employ reasonable security measures under Section 5 of the FTC 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.

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

180. For instance, HIPAA required Defendant to notify victims of the Breach within 60 days of the discovery of the Data Breach. Defendant did not begin to notify Plaintiffs or Class Members of the Data Breach until June 18, 2024 despite Defendant having known since at least February 12, 2024 that its patients' data had been compromised. Similarly, HIPAA required Defendant, *inter alia*, to act promptly. However, despite learning of the breach on February 12, 2024, CRL's investigation did not conclude until April 17, 2024.[54]

181. Defendant owed a duty of care to Plaintiffs and Class Members to provide data security consistent with industry standards and other requirements discussed herein,

[54] *See* Ex. A.

and to ensure that its systems and networks, and the personnel responsible for them, adequately protected the Private Information.

182. Defendant's duty of care to use reasonable security measures arose as a result of the special relationship that existed between Defendant and its patients. That special relationship arose because Plaintiffs and the Class ultimately entrusted Defendant with their confidential Private Information, a necessary part of being patients of CRL.

183. 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.

184. Defendant was subject to an "independent duty," untethered to any contract between Defendant and Plaintiffs or the Class.

185. Defendant also had a duty to exercise appropriate practices to remove Private Information once it was no longer required to retain pursuant to regulations.

186. Moreover, Defendant had a duty to promptly and adequately notify Plaintiffs and the Class of the Data Breach.

187. Defendant had and continues to have a duty to adequately disclose that the Private Information of Plaintiffs and the Class within Defendant's possession might have been compromised, how it was compromised, and precisely the types of data that were compromised and when. Such notice was necessary to allow Plaintiffs and the Class to take steps to prevent, mitigate, and repair any identity theft and the fraudulent use of their Private Information by third parties.

188. Defendant breached its duties, pursuant to the FTC Act, HIPAA, and other applicable standards, and thus were negligent, by failing to use reasonable measures to protect Class Members' Private Information. The specific negligent acts and omissions committed by Defendant include, but are not limited to, the following:

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

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

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

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

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

f. Failing to remove former patients' and employees' Private Information it was no longer required to retain pursuant to regulations,

g. Failing to timely and adequately notify Class Members about the Data Breach's occurrence and scope, so that they could take appropriate steps to mitigate the potential for identity theft and other damages; and

h. Failing to secure its stand-alone personal computers, such as the reception desk computers, even after discovery of the data breach.

189. Defendant violated Section 5 of the FTC Act and HIPAA by failing to use reasonable measures to protect Private Information and not complying with applicable industry standards, as described in detail herein. Defendant's conduct was particularly

unreasonable given the nature and amount of Private Information it obtained and stored and the foreseeable consequences of the immense damages that would result to Plaintiffs and the Class.

190. Plaintiffs and the Class are within the class of persons that the FTC Act and HIPAA were intended to protect.

191. The harm that occurred as a result of the Data Breach is the type of harm the FTC Act and HIPAA were intended to guard against.

192. Defendant's violations of Section 5 of the FTC Act and HIPAA constitute negligence.

193. The FTC has pursued enforcement actions against businesses, which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiffs and the Class.

194. A breach of security, unauthorized access, and resulting injury to Plaintiffs and the Class was reasonably foreseeable, particularly in light of Defendant's inadequate security practices.

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

196. Defendant has full knowledge of the sensitivity of the Private Information and the types of harm that Plaintiffs and the Class could and would suffer if the Private Information were wrongfully disclosed.

197. Plaintiffs and the Class were the foreseeable and probable victims of any inadequate security practices and procedures. Defendant knew or should have known of the inherent risks in collecting and storing the Private Information of Plaintiffs and the Class, the critical importance of providing adequate security of that Private Information, and the necessity for encrypting Private Information stored on Defendant's systems.

198. It was therefore foreseeable that the failure to adequately safeguard Class Members' Private Information would result in one or more types of injuries to Class Members.

199. Plaintiffs and the Class had no ability to protect their Private Information that was in, and possibly remains in, Defendant's possession.

200. Defendant was in a position to protect against the harm suffered by Plaintiffs and the Class as a result of the Data Breach.

201. Defendant's duty extended to protecting Plaintiffs and the Class from the risk of foreseeable criminal conduct of third parties, which has been recognized in situations where the actor's own conduct or misconduct exposes another to the risk or defeats protections put in place to guard against the risk, or where the parties are in a special relationship. *See* Restatement (Second) of Torts § 302B. Numerous courts and legislatures have also recognized the existence of a specific duty to reasonably safeguard personal information.

202. Defendant has admitted that the Private Information of Plaintiffs and the Class was wrongfully lost and disclosed to unauthorized third persons as a result of the Data Breach.

203. But for Defendant's wrongful and negligent breach of duties owed to Plaintiffs and the Class, the Private Information of Plaintiffs and the Class would not have been compromised.

204. There is a close causal connection between Defendant's failure to implement security measures to protect the Private Information of Plaintiffs and the Class and the harm, or risk of imminent harm, suffered by Plaintiffs and the Class. The Private Information of Plaintiffs and the Class was lost and accessed as the proximate result of Defendant's failure to exercise reasonable care in safeguarding such Private Information by adopting, implementing, and maintaining appropriate security measures.

205. As a direct and proximate result of Defendant's negligence, Plaintiffs and the Class have suffered and will suffer injury, including but not limited to: (i) invasion of privacy; (ii) theft of their Private Information; (iii) lost or diminished value of Private Information; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) experiencing an increase in spam calls, texts, and/or emails; (viii) statutory damages; (ix) nominal damages; and (x) the continued and certainly increased risk to their Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up 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.

206. As a direct and proximate result of Defendant's negligence, Plaintiffs and the Class have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

207. Additionally, as a direct and proximate result of Defendant's negligence, Plaintiffs and the Class have suffered and will suffer the continued risks of exposure of their Private Information, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information in its continued possession.

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

209. Defendant's negligent conduct is ongoing, in that it still holds the Private Information of Plaintiffs and Class Members in an unsafe and insecure manner.

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

SECOND CAUSE OF ACTION
NEGLIGENCE PER SE
(On Behalf of Plaintiffs and the Class)

211. Plaintiffs repeat, re-allege, and incorporate by reference, all other paragraphs of this complaint.

212. Section 5 of the FTC Act, 15 U.S.C. § 45, prohibits "unfair . . . practices in or affecting commerce" including, as interpreted and enforced by the FTC, the unfair act or practice by Defendant of failing to use reasonable measures to protect Private Information. Various FTC publications and orders also form the basis of Defendant's duty.

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

214. For instance, HIPAA required Defendant to notify victims of the Breach within 60 days of the discovery of the Data Breach. CRL did not begin to notify Plaintiffs or Class Members of the Data Breach until June 18, 2024 despite Defendant having known since at least February 12, 2024 that its patients' data had been compromised. Similarly, HIPAA required Defendant, *inter alia*, to act promptly. However, despite learning of the breach on February 12, 2024, CRL's investigation did not conclude until April 17, 2024.[55]

215. Defendant violated Section 5 of the FTC Act, HIPAA, and similar state statutes by failing to use reasonable measures to protect Private Information and not complying with industry standards. Defendant's conduct was particularly unreasonable

[55] *See* Ex. A.

given the nature and amount of Private Information obtained and stored and the foreseeable consequences of a data breach on its systems.

216. Defendant's violation of Section 5 of the FTC Act, HIPAA, and similar state statutes constitutes negligence *per se*.

217. Class Members are consumers within the class of persons Section 5 of the FTC Act, HIPAA, and similar state statutes were intended to protect.

218. Moreover, the harm that has occurred is the type of harm the FTC Act, HIPAA, and similar state statutes were intended to guard against. Indeed, the FTC has pursued over fifty enforcement actions against businesses which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm suffered by Plaintiffs and Class Members.

219. As a direct and proximate result of Defendant's conduct, Plaintiffs and Class Members have suffered or will suffer injury, including but not limited to: (i) invasion of privacy; (ii) theft of their Private Information; (iii) lost or diminished value of Private Information; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) statutory damages; (viii) nominal damages; and (ix) the continued and certainly increased risk to their Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up 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.

220. Plaintiffs and Class Members have been injured and are entitled to damages in an amount to be proven at trial.

THIRD CAUSE OF ACTION
BREACH OF IMPLIED CONTRACT
(On Behalf of Plaintiffs and the Class)

221. Plaintiffs repeat, re-allege, and incorporate by reference, all other paragraphs of this complaint.

222. Plaintiffs and the Class ultimately entrusted their Private Information to Defendant. In so doing, Plaintiffs and the Class entered into implied contracts with Defendant by which Defendant agreed to safeguard and protect such information, to keep such information secure and confidential, and to timely and accurately notify Plaintiffs and the Class if their data had been breached and compromised or stolen.

223. In its Privacy Policy posted on its website, Defendant represented that with respect to information its patients provide to it, CRL would "work hard to protect the privacy of [its patients'] health information," and that it "ha[s] rules for [its] employees on how to manage this information."[56]

224. Plaintiffs and the Class fully performed their obligations under the implied contracts with Defendant.

[56] https://consultingradiologists.com/resources/hipaa-privacy-policy/ (last accessed June 26, 2024).

225. When Plaintiffs and Class Members provided their Private Information to Defendant in exchange for services, they entered into protect such information and to destroy any Private Information that it was no longer required to maintain.

226. The mutual understanding and intent of Plaintiffs and Class Members on the one hand, and Defendant on the other, is demonstrated by their conduct and course of dealing.

227. Defendant solicited, offered, and invited Plaintiffs and Class Members to provide their Private Information as part of Defendant's regular business practices.

228. Plaintiffs and Class Members accepted Defendant's offers and provided their Private Information to Defendant.

229. In accepting the Private Information of Plaintiffs and Class Members, Defendant understood and agreed that it was required to reasonably safeguard the Private Information from unauthorized access or disclosure.

230. In entering into such implied contracts, Plaintiffs and Class Members reasonably believed and expected that Defendant's data security practices complied with relevant laws and regulations, including HIPAA, the FTC Act, and were consistent with industry standards.

231. As a result of services contracted by Plaintiffs and Class Members, Defendant earned money with the reasonable belief and expectation that Defendant would use part of its earnings to obtain adequate data security. Defendant failed to do so.

232. Plaintiffs and Class Members would not have entrusted their Private Information to Defendant in the absence of the implied contract between them and Defendant to keep their information reasonably secure.

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

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

235. Defendant breached its implied contracts with Plaintiffs and Class Members by failing to safeguard and protect their Private Information or to destroy it once it was no longer necessary to retain the Private Information.

236. As a direct and proximate result of Defendant's breach of the implied promises, Plaintiffs and Class Members are at a current and ongoing risk of identity theft, and Plaintiffs and Class Members sustained incidental and consequential damages including: (a) financial "out of pocket" costs incurred mitigating the materialized risk and imminent threat of identity theft; (b) loss of time and loss of productivity incurred mitigating the materialized risk and imminent threat of identity theft risk; (c) financial "out of pocket" costs incurred due to actual identity theft; (d) spam and targeted marketing emails; (e) diminution of value of their Private Information; (f) future costs of identity theft monitoring; (g) and the continued risk to their Private Information, which remains in Defendant's possession, and which is subject to further breaches, so long as Defendant fails

to undertake appropriate and adequate measures to protect Plaintiffs' and Class Members' Private Information.

237. Plaintiffs and Class Members are entitled to compensatory, consequential, and nominal damages suffered as a result of the Data Breach to be determined at trial.

238. 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.

FOURTH CAUSE OF ACTION
UNJUST ENRICHMENT
[In the Alternative]
(On Behalf of Plaintiffs and the Class)

239. Plaintiffs repeat, re-allege, and incorporate by reference, all other paragraphs of this complaint.

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

241. Plaintiffs and Class Members conferred a benefit on Defendant. Specifically, they provided Defendant with their Private Information. In exchange, Plaintiffs and Class Members should have had their Private Information protected with adequate data security.

242. Defendant knew that Plaintiffs and Class Members conferred a benefit on it in the form of their Private Information. Defendant appreciated and accepted that benefit. Defendant profited from these transactions and used the Private Information of Plaintiffs and Class Members for business purposes.

243. Upon information and belief, Defendant funds its data security measures entirely from its general revenue, including payments on behalf of or for the benefit of Plaintiffs and some Class Members.

244. As such, a portion of the payments made for the benefit of or on behalf of Plaintiffs and Class Members is to be used to provide a reasonable level of data security, and the amount of the portion of each payment made that is allocated to data security is known to Defendant.

245. Defendant, however, failed to secure Plaintiffs' and Class Members' Private Information and, therefore, did not provide adequate data security in return for the benefit Plaintiffs and Class Members provided.

246. Defendant would not be able to carry out an essential function of its regular business without the Private Information of Plaintiffs and Class Members and derived revenue by using it for business purposes. Plaintiffs and Class Members expected that Defendant or anyone in Defendant's position would use a portion of that revenue to fund adequate data security practices.

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

248. If Plaintiffs and Class Members knew that Defendant had not reasonably secured their Private Information, they would not have allowed their Private Information to be provided to Defendant.

249. Defendant enriched itself by saving the costs it reasonably should have expended on data security measures to secure Plaintiffs' and Class Members' Private

Information. Instead of providing a reasonable level of security that would have prevented the hacking incident, Defendant instead calculated to increase its own profit at the expense of Plaintiffs and Class Members by utilizing cheaper, ineffective security measures and diverting those funds to its own profit. Plaintiffs and Class Members, on the other hand, suffered as a direct and proximate result of Defendant's decisions to prioritize their own profits over the requisite security and the safety of their Private Information.

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

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

252. As a direct and proximate result of Defendant's conduct, Plaintiffs and Class Members have suffered and will suffer injury, including but not limited to: (i) invasion of privacy; (ii) theft of their Private Information; (iii) lost or diminished value of Private Information; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) experiencing an increase in spam calls, texts, and/or emails; (viii) statutory damages; (ix) nominal damages; and (x) the continued and certainly increased risk to their Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up 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.

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

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

FIFTH CAUSE OF ACTION
DECLARATORY JUDGMENT AND INJUNCTIVE RELIEF
(On Behalf of Plaintiffs and the Class)

255. Plaintiffs repeat, re-allege, and incorporate by reference, all other paragraphs of this complaint.

256. Under the Declaratory Judgment Act, 28 U.S.C. §§ 2201, *et seq*., this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and to grant further necessary relief. Furthermore, the Court has broad authority to restrain acts, such as those alleged herein, which are tortious, and which violate the terms of the federal and state statutes described above.

257. An actual controversy has arisen in the wake of the Data Breach at issue regarding Defendant's common law and other duties to act reasonably with respect to employing reasonable data security. Plaintiffs allege Defendant's actions in this respect were inadequate and unreasonable and, upon information and belief, remain inadequate and unreasonable. Additionally, Plaintiffs and the Class continue to suffer injury due to the

continued and ongoing threat of new or additional fraud against them or on their accounts using the stolen data.

258. Under its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following: Defendant owed, and continues to owe, a legal duty to employ reasonable data security to secure the Private Information it possesses, and to notify impacted individuals of the Data Breach under the common law and Section 5 of the FTC Act; Defendant breached, and continues to breach, its duty by failing to employ reasonable measures to secure its customers' personal and financial information; and Defendant's breach of its legal duty continues to cause harm to Plaintiffs and the Class.

259. The Court should also issue corresponding injunctive relief requiring Defendant to employ adequate security protocols consistent with industry standards to protect its employees' (i.e., Plaintiffs' and the Class's) data.

260. 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 breach of Defendant's data systems. If another breach of Defendant's data systems occurs, Plaintiffs and the Class will not have an adequate remedy at law because many of the resulting injuries are not readily quantified in full and they will be forced to bring multiple lawsuits to rectify the same conduct. Simply put, monetary damages, while warranted to compensate Plaintiffs and the Class for their out-of-pocket and other damages that are legally quantifiable and provable, do not cover the full extent of injuries suffered by Plaintiffs and the Class, which include monetary damages that are not legally quantifiable or provable.

261. The hardship to Plaintiffs and the Class if an injunction is not issued exceeds the hardship to Defendant if an injunction is issued.

262. 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, thus eliminating the injuries that would result to Plaintiffs, the Class, and the public at large.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, on behalf of themselves and Class Members, request judgment against Defendant and that the Court grant the following:

a) Certification of this action as a class action and appointing Plaintiffs and their counsel to represent the Class;

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

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

d) Injunctive relief requested by Plaintiffs, including but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Plaintiffs and Class Members;

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

f) An Order requiring Defendant to pay for not less than ten years of credit monitoring services for Plaintiffs and the Class;

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

h) An award of punitive damages, as allowable by law;

i) An award of attorneys' fees and costs, and any other expense, including expert witness fees;

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

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

DEMAND FOR JURY TRIAL

Plaintiffs hereby demand that this matter be tried before a jury.

Respectfully submitted,

Date: July 1, 2024

/s/ Brian C. Gudmundson

Brian C. Gudmundson (MN Bar No. 336695)
Michael J. Laird (MN Bar No. 394836)
Rachel K. Tack (MN Bar No. 399529)
ZIMMERMAN REED LLP
1100 IDS Center
80 South 8th Street
Minneapolis, MN 55402
Telephone: (612) 341-0400
brian.gudmundson@zimmreed.com
michael.laird@zimmreed.com
rachel.tack@zimmreed.com

Jeffrey S. Goldenberg (*pro hac vice* forthcoming)
GOLDENBERG SCHNEIDER, LPA
4445 Lake Forest Drive, Suite 490
Cincinnati, OH 45242
Telephone: (513) 345-8291
jgoldenberg@gs-legal.com