UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF OHIO
EASTERN DIVISION

In re Red Roof Inns, Inc. Data Incident Litigation	Case No. 2:23-cv-4133 Judge Sarah D. Morrison Magistrate Judge Chelsey M. Vascura

CONSOLIDATED CLASS ACTION COMPLAINT

Plaintiffs Rebecca Richardson, Vail Pinkston McCall, and Viomar Sena (collectively, "Plaintiffs") bring this Consolidated Class Action Complaint against Red Roof Inns, Inc. ("Red Roof" or "Defendant"), individually and behalf of all others similarly situated ("Class Members"), and allege, upon personal knowledge as to their own actions and their counsels' investigations, and upon information and belief as to all other matters, as follows:

INTRODUCTION

1. This class action arises out of the recent targeted cyberattack and data breach on Red Roof's network on or around September 21, 2023, and September 23, 2023 that resulted in unauthorized access to highly sensitive employee data, including that of current and former employees (the "Data Breach").

2. As a result of Defendant's failure to adequately secure the personal information it demanded from its current, former, and prospective employees, Plaintiffs and more than 27,000 other Class Members had their highly sensitive personal information accessed and exfiltrated by cybercriminals.

3. The data compromised in this Data Breach includes personally identifiable information ("PII") like names; dates of birth; Social Security numbers; driver's license numbers; driver's license states; state ID numbers; U.S. alien registration numbers; passport numbers; bank

account numbers; routing numbers; financial documents with account numbers; credit and/or debit card numbers, expiration dates, and security codes and pins, and protected health information ("PHI"), such as health insurance information and medical information (collectively "PHI"). Upon information and belief, the data compromised also included contact information, such as residential addresses, email addresses, and phone numbers, as such information would have been routinely stored with the other data impacted in the Data Breach, e.g., financial documents and health insurance information. The PII and PHI that Defendant collected and maintained is collectively referred to herein as "Private Information."

4. Following its discovery of the Data Breach, Defendant then waited roughly three months to notify victims of the Data Breach like Plaintiffs that their Private Information was stolen and now in the hands of cybercriminals.

5. Armed with the Private Information accessed in the Data Breach, data thieves have or will commit a variety of crimes, including opening new financial accounts in Class Members' names, obtaining driver's licenses in Class Members' names but with another person's photograph, taking out loans in Class Members' names, using Class Members' information to obtain government benefits and/or medical services, filing fraudulent tax returns using Class Members' information, targeting Plaintiffs and Class Members with phishing and spam communications, and giving false information to police during an arrest, among other offenses.

6. Defendant maintained Plaintiffs' and Class Members' Private Information in a negligent and/or reckless manner. Particularly, Defendant's computer system and network in which it maintained the Private Information was insufficient such that it left it vulnerable to cyberattacks. Upon information and belief, the mechanism of the cyberattack and potential for improper disclosure of Plaintiffs' and Class Members' Private Information was known to

Defendant, and thus Defendant was on notice for failing to take the necessary steps to secure the Private Information and remedy those risks.

7. Additionally, upon information and belief, Red Roof and its employees failed to encrypt the Private Information that it stored in an internet accessible manner and failed to properly monitor the computer network and IT systems that housed the Private Information.

8. Plaintiffs' and Class Members' identities remain at risk because of Defendant's negligent conduct because the Private Information collected and maintained by Red Roof is now in the hands of data thieves.

9. As a result of the Data Breach, Plaintiffs and Class Members have been exposed to a present and continuing threat of fraud and identity theft. Plaintiffs and Class Members must now—and indefinitely—closely monitor their financial accounts and credit to guard against identity theft.

10. Plaintiffs bring this action against Defendant seeking redress for the injuries through claims for: (1) negligence; (2) negligence *per se* (3) breach of implied contract; (4) invasion of privacy; (5) unjust enrichment; (6) declaratory judgment.

THE PARTIES

11. Plaintiff McCall is a natural person, resident, and a citizen of the State of Florida, where she intends to remain. Plaintiff McCall received a notice letter from Defendant dated December 8, 2023, explaining that in September 2023, her Private Information was compromised in a Data Breach.

12. Plaintiff Sena is a natural person, resident, and a citizen of the State of New Jersey, where she intends to remain. Plaintiff Sena received a notice letter from Defendant dated December 8, 2023, explaining that in September 2023, her Private Information was compromised

in a Data Breach.

13. Plaintiff Richardson is a natural person, resident, and a citizen of the State of Missouri, where she intends to remain. Plaintiff Richardson received a notice letter from Defendant dated December 8, 2023, explaining that in September 2023, her Private Information was compromised in a Data Breach.

14. Defendant Red Roof Inns, Inc. is a New Albany, Ohio-based economy hotel chain with over 600 properties globally, primarily in the Midwest, Southern, and Eastern United States, that employs over 4,000 people and generates approximately $990 million in annual revenue.

JURISDICTION AND VENUE

15. This Court has general personal jurisdiction over Defendant Red Roof because Red Roof maintains its principal place of business at 7815 Walton Parkway, New Albany, Ohio; regularly conducts business in Ohio; and has sufficient minimum contacts in Ohio.

16. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(b) because Red Roof's principal place of business is in this District and a substantial part of the events, acts, and omissions giving rise to Plaintiffs' claims occurred in this District.

DEFENDANT'S BUSINESS

17. As a condition of employment with Defendant, Defendant requires that its employees entrust it with highly sensitive personal information.

18. In the ordinary course of employment with Red Roof, Plaintiffs and Class Members were required to provide their Private Information to Defendant and did so on the understanding that Red Roof would maintain it as confidential and secure from cyber intrusions.

19. Defendant's Privacy Policy provides that Red Roof "knows that your privacy and

information security is important to you."[1]

20. Defendant's Privacy Policy states, "Red Roof collects a variety of information such as information directly provided to us by Site visitors, hotel guests, and job applicants. We also collect information about our Site users through cookies, digital footprints, third parties, and data analytic sources."[2]

21. Defendant also promises, "The security of Personal Information is very important to us, and we are committed to protecting the Information we collect. We collect Information only in a manner deemed reasonably necessary to serve our legitimate business purposes and comply with our legal obligations."[3]

22. Upon information and belief, in the ordinary course of its business, Red Roof maintains the Private Information of its employees, including but not limited to:

- Name, address, phone number, and email address;
- Date of birth;
- Demographic information;
- Social Security number;
- Financial information;
- Information relating to individual medical history;
- Information concerning an individual's doctor, nurse, or other medical providers;
- Medication information;

[1] Red Roof Inn, Privacy Policy, https://www.redroof.com/privacy-policy (last visited April 15, 2024).
[2] *Id.*
[3] *Id.*

- Photo identification;
- Employment information, and;
- Other information that Defendant may deem necessary in the course of its employment relationship.

23. Because of the highly sensitive and personal nature of the Private Information Defendant acquires and stores with respect to employees, Red Roof, upon information and belief, promises to, among other things: keep protected health information private; comply with industry standards related to data security and Private Information; inform employees of its legal duties and comply with all federal and state laws protecting employee and patient Private Information; only use and release Private Information for reasons that relate to Red Roof's business; and provide adequate notice to individuals if their Private Information is disclosed without authorization.

24. By obtaining, collecting, using, and deriving a benefit from Plaintiffs' and Class Members' Private information, Defendant assumed legal and equitable duties and knew—or should have known—that it was responsible for protecting Plaintiffs' and Class Members' Private Information from unauthorized disclosure.

25. Plaintiffs and Class Members have taken reasonable steps to maintain the confidentiality of their Private Information.

26. Plaintiffs and Class Members relied on defendant to implement and follow adequate data security policies and protocols; to keep their Private Information confidential and secure; to use such Private Information solely for business purposes; and to prevent unauthorized disclosures of Private Information.

THE CYBERATTACK

27. On or about September 23, 2023 Red Roof detected a cyber-attack that it "identified

as bearing the hallmarks of a ransomware attack, including the encryption of a limited subset of Red Roof data."[4] During the attack, the threat actor gained access to and "copied" the Private Information of Plaintiffs and Class Members. Recognizing the imminent threat of identity theft and fraud resulting from the Data Breach, Defendant admonished Plaintiffs and Class Members "to remain vigilant against incidents of identity theft and fraud by reviewing their account statements and monitoring their free credit reports for suspicious activity."[5]

28. Through this investigation, Red Roof determined that the cyber-attack impacted its network, resulting in the unauthorized access and acquisition of the highly sensitive information being stored thereon.

29. Red Roof determined that the categories of personal information in the copied data included names, dates of birth, social security numbers, driver's license numbers, passport numbers, financial account numbers, credit and/or debit card numbers, medical information, and health insurance information.

30. Red Roof's investigation further concluded that at least 27,327 individuals—including Plaintiffs—were victims of the Data Breach.

31. Red Roof waited until December 8, 2023 to begin notifying victims that their Private Information was compromised in the Data Breach.

32. When Defendant finally notified Plaintiffs and Class Members of the Data Breach, Defendant acknowledged that the Data Breach created a present, continuing, and significant risk of identity theft and other consequences, warning Plaintiffs and Class Members to:

a. "remain vigilant against incidents of identity theft and fraud by reviewing your

[4] https://www.prnewswire.com/news-releases/red-roof-provides-notice-of-security-incident-302010510.html
[5] *Id*.

account statements and monitoring your free credit reports for suspicious activity and to detect errors;"

b. "enroll in the credit monitoring and identity protection services;"

c. "place a fraud alert in your file by calling on of the three nationwide credit reporting agencies;" and

d. "obtain information about steps to take to avoid identity theft from the Federal Trade Commission."[6]

33. On information and belief, Plaintiffs' and Class Members' Private Information was sold on the dark web following the Data Breach, as that is the *modus operandi* of cybercriminals. Indeed, Plaintiff McCall's Private Information has already been located on the dark web by Experian.

34. As the United States Cybersecurity and Infrastructure Security Agency recognizes, "[m]ore than 90% of all cyber attacks begin with phishing."[7] Upon information and belief, the cybercriminals were able to first gain access to Red Roof's network through rudimentary phishing or other social engineering techniques. This means that Defendant affirmatively, albeit negligently or recklessly under false pretenses, provided cybercriminals with direct access to Plaintiffs' and Class Members' Private Information.

35. Defendant had obligations created by contract, industry standards, common law, and/or its own promises and representations made to Plaintiffs and Class Members to keep their

[6] Red Roof Inns, Inc., Notice of Data Breach, https://apps.web.maine.gov/online/aeviewer/ME/40/8a9ff5c2-9ff4-4f8e-bbdf-987d931364c5.shtml (last visited April 14, 2024).

[7] https://www.cisa.gov/stopransomware/general-information#:~:text=Fend%20Off%20Phishing%20%3A%20Learn%20how,to%20better%20recognize%20phishing%20emails. (last visited April 29, 2024).

Private Information confidential and to protect it from unauthorized access and disclosure.

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

37. Defendant's data security obligations were particularly critical given the substantial increase in cyberattacks and/or data breaches in the industry preceding the date of the breach.

38. Considering recent high profile data breaches at other hotel and motel companies, Defendant knew or should have known that their electronic records and employee Private Information would be targeted by cybercriminals and ransomware attack groups.

39. The increase in such attacks, and the attendant risk of future attacks, was widely known to the public and anyone in Defendant's industry, Defendant included.

DEFENDANT FAILS TO COMPLY WITH FTC GUIDELINES

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

41. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established cyber-security guidelines for businesses. The guidelines note that businesses should protect the personal 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.[8] The guidelines also recommend that businesses use an intrusion detection system to

[8] *Protecting Personal Information: A Guide for Business*, Federal Trade Commission (2016).

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.[9]

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

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

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

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

46. Defendant was at all times fully aware of its obligation to protect the Private Information of customers and employees. Defendant was also aware of the significant repercussions that would result from its failure to do so.

Available at https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last visited April 15, 2024).

[9] *Id*.

DEFENDANT FAILS TO COMPLY WITH INDUSTRY STANDARDS

47. As discussed herein, experts studying cybersecurity routinely identify companies in the hotel and hospitality industry as being particularly vulnerable to cyberattacks because of the value of the Private Information which they collect and maintain.

48. Several best practices have been identified that at a minimum should be implemented by Defendant, including but not limited to; educating all employees; strong passwords; multi-layer security, including firewalls, anti-virus, and anti-malware software; encryption, making data unreadable without a key; multi-factor authentication; backup data; and limiting which employees can access sensitive data.

49. Other best cybersecurity practices that are standard in the hospitality industry include installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches and routers; monitoring and protection of physical security systems; protection against any possible communication system; training staff regarding critical points.

50. 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.

51. These foregoing frameworks are existing and applicable industry standards in the hospitality industry, and Defendant failed to comply with these accepted standards, thereby opening the door to the cyber incident and causing the data breach.

DEFENDANT'S DATA BREACH WAS PREVENTABLE

52. Defendant could have prevented this Data Breach by, among other things, properly encrypting or otherwise protecting their equipment and computer files containing Private Information. Defendant could also have employed multi-factor authentication to ensure that compromised passwords could not be used by unauthorized individuals.

53. A ransomware attack is a type of cyberattack that is frequently used to target healthcare providers due to the sensitive patient data they maintain.[10] In a ransomware attack the attackers use software to encrypt data on a compromised network, rendering it unusable and demanding payment to restore control over the network.[11]

54. Companies should treat ransomware attacks as any other data breach incident because ransomware attacks don't just hold networks hostage, "ransomware groups sell stolen data in cybercriminal forums and dark web marketplaces for additional revenue."[12] As cybersecurity expert Emisoft warns, "[a]n absence of evidence of exfiltration should not be construed to be evidence of its absence […] the initial assumption should be that data may have been exfiltrated."

55. An increasingly prevalent form of ransomware attack is the "encryption+exfiltration" attack in which the attacker encrypts a network and exfiltrates the data contained within.[13] In 2020, over 50% of ransomware attackers exfiltrated data from a network

---

[10] *Ransomware warning: Now attacks are stealing data as well as encrypting it*, available at https://www.zdnet.com/article/ransomware-warning-now-attacks-are-stealing-data-as-well-as-encrypting-it/

[11] *Ransomware FAQs*, available at https://www.cisa.gov/stopransomware/ransomware-faqs

[12] *Ransomware: The Data Exfiltration and Double Extortion Trends*, available at https://www.cisecurity.org/insights/blog/ransomware-the-data-exfiltration-and-double-extortion-trends

[13] *The chance of data being stolen in a ransomware attack is greater than one in ten*, available at https://blog.emsisoft.com/en/36569/the-chance-of-data-being-stolen-in-a-ransomware-attack-is-greater-than-one-in-ten/

before encrypting it.[14] Once the data is exfiltrated from a network, its confidential nature is destroyed and it should be "assume[d] it will be traded to other threat actors, sold, or held for a second/future extortion attempt."[15] And even where companies pay for the return of data attackers often leak or sell the data regardless because there is no way to verify copies of the data are destroyed.[16]

56. As explained by the Federal Bureau of Investigation, "[p]revention is the most effective defense against ransomware and it is critical to take precautions for protection."[17]

57. 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.

---

[14] 2020 Ransomware Marketplace Report, available at https://www.coveware.com/blog/q3-2020-ransomware-marketplace-report
[15] *Id*.
[16] *Id*.
[17] 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

- Set anti-virus and anti-malware programs to conduct regular scans automatically.
- Manage the use of privileged accounts based on the principle of least privilege: no users should be assigned administrative access unless absolutely needed; and those with a need for administrator accounts should only use them when necessary.
- Configure access controls—including file, directory, and network share permissions—with least privilege in mind. If a user only needs to read specific files, the user should not have write access to those files, directories, or shares.
- Disable macro scripts from office files transmitted via email. Consider using Office Viewer software to open Microsoft Office files transmitted via email instead of full office suite applications.
- Implement Software Restriction Policies (SRP) or other controls to prevent programs from executing from common ransomware locations, such as temporary folders supporting popular Internet browsers or compression/decompression programs, including the AppData/LocalAppData folder.
- Consider disabling Remote Desktop protocol (RDP) if it is not being used.
- Use application whitelisting, which only allows systems to execute programs known and permitted by security policy.
- Execute operating system environments or specific programs in a virtualized environment.
- Categorize data based on organizational value and implement physical and logical separation of networks and data for different organizational units.[18]

58. 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;

[18] *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
- Turn on attack surface reduction rules and [Antimalware Scan Interface] for Office [Visual Basic for Applications].[19]

59. Given that Defendant was storing the Private Information of its current and former employees, Defendant could and should have implemented all of the above measures to prevent and detect cyberattacks.

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

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

and data thieves acquiring and accessing the Private Information of, upon information and belief, thousands to tens of thousands of individuals, including that of Plaintiffs and Class Members.

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

a. Failing to maintain an adequate data security system to reduce the risk of data breaches and cyber-attacks;

b. Failing to adequately protect employees' Private Information;

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

d. Failing to ensure that its vendors with access to its computer systems and data employed reasonable security procedures;

e. Failing to train its employees in the proper handling of emails containing Private Information and maintain adequate email security practices;

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

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

h. Otherwise breaching its duties and obligations to protect Plaintiffs' and Class Members' Private Information.

62. Following the Data Breach, Defendant has stated that it "implemented measures to further improve the security of Red Roof's information technology systems and practices, including implementing software and hardware to prevent, detect, and respond to unauthorized activity, resetting and strengthening passwords, implementing new risk management protocols,

and adopting new network access policies."[20] These are all things that a reasonable entity in Red Roof's position would have done before the Data Breach.

63. Upon information and belief, the number of Data Breach victims far exceeds the number of active Red Roof Inn employees, indicating that Red Roof Inn maintained Private Information on its network for far longer than it had legitimate use for.

64. Defendant negligently and unlawfully failed to safeguard Plaintiffs' and Class Members' Private Information by allowing cyberthieves to access Red Roof's computer network and systems which contained unsecured and unencrypted Private Information.

65. Accordingly, as outlined below, Plaintiffs and Class Members now face an increased risk of fraud and identity theft. In addition, Plaintiffs and the Class Members also lost the benefit of the bargain they made with Defendant.

CYBERATTACKS AND DATA BREACHES CAUSE DISRUPTION AND PUT INDIVIDUALS AT AN INCREASED RISK OF FRAUD AND IDENTITY THEFT

66. Cyberattacks and data breaches at hospitality companies like Defendant are especially problematic because they can negatively impact the overall daily lives of individuals affected by the attack.

67. That is because any victim of a data breach is exposed to serious ramifications regardless of the nature of the data. Indeed, the reason criminals steal personally identifiable information is to monetize it. They do this by selling the spoils of their cyberattacks on the black market to identity thieves who desire to extort and harass victims, take over victims' identities to engage in illegal financial transactions under the victims' names. Because a person's identity is akin to a puzzle, the more accurate pieces of data an identity thief obtains about a person, the easier

[20] https://www.prnewswire.com/news-releases/red-roof-provides-notice-of-security-incident-302010510.html (last visited April 23, 2024).

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

68. One such example of criminals piecing together bits and pieces of compromised Private Information for profit is the development of "Fullz" packages.[21]

69. 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.

70. 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

[21] "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/

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

71. 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 insurance information) of Plaintiffs and the other Class Members.

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

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

74. The FTC recommends that identity theft 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 7 years if someone steals their identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.[22]

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

76. Identity thieves can also use Social Security numbers to obtain a driver's license or

[22] *See IdentityTheft.gov*, Federal Trade Commission, https://www.identitytheft.gov/Steps (last visited April 15, 2024).

official identification card in the victim's name but with the thief's picture; use the victim's name and Social Security number to obtain government benefits; or file a fraudulent tax return using the victim's information. In addition, identity thieves may obtain a job using the victim's Social Security number, rent a house or receive medical services in the victim's name, target victims through sophisticated phishing attacks, and may even give the victim's personal information to police during an arrest resulting in an arrest warrant being issued in the victim's name.

77. Moreover, theft of Private Information is also gravely serious because Private Information is an extremely valuable property right.[23]

78. Its value is axiomatic, considering the value of "big data" in corporate America and the fact that the consequences of cyber thefts include heavy prison sentences. Even this obvious risk to reward analysis illustrates beyond doubt that Private Information has considerable market value.

79. Theft of PHI, in particular, is gravely serious: "[a] thief may use your name or health insurance numbers to see a doctor, get prescription drugs, file claims with your insurance 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]

80. Drug manufacturers, medical device manufacturers, pharmacies, hospitals, and other healthcare service providers often purchase Private Information on the black market for the purpose of target marketing their products and services to the physical maladies of the data breach

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

[24] *See* Federal Trade Commission, *Medical Identity Theft*, http://www.consumer.ftc.gov/articles/0171-medical-identity-theft (last visited April 15, 2024).

victims themselves. Insurance companies purchase and use wrongfully disclosed PHI to adjust their insureds' medical insurance premiums.

81. "Medical identity theft is a growing and dangerous crime that leaves its victims with little to no recourse for recovery," reported Pam Dixon, executive director of World Privacy Forum. "Victims often experience financial repercussions and worse yet, they frequently discover erroneous information has been added to their personal medical files due to the thief's activities."[25]

82. 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.[26] 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.[27]

83. It must also be noted there may be a substantial time lag – measured in years - between when harm occurs and when it is discovered, and also between when Private Information and/or financial information is stolen and when it is used.

84. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent

[25] Michael Ollove, "The Rise of Medical Identity Theft in Healthcare," Kaiser Health News, Feb. 7, 2014, https://khn.org/news/rise-of-indentity-theft/ (last accessed July 24, 2023).
[26] *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/ (last accessed July 24, 2023).
[27] *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/ (last accessed July 24, 2023).

> use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.

See GAO Report, at p. 29.

85. Private Information is such a valuable commodity to identity thieves that once the information has been compromised, criminals often trade the information on the "cyber black-market" for years.

86. There is a strong probability that entire batches of stolen information have been dumped on the black market and are yet to be dumped on the black market, meaning Plaintiffs and Class Members are at an increased risk of fraud and identity theft for many years into the future.

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

88. Private Information can sell for as much as $363 per record according to the Infosec Institute.[28] PII is particularly valuable because criminals can use it to target victims with frauds and scams. Once PII is stolen, fraudulent use of that information and damage to victims may continue for years.

89. For example, the Social Security Administration has warned that identity thieves can use an individual's Social Security number to apply for additional credit lines.[29] Such fraud may go undetected until debt collection calls commence months, or even years, later. Stolen Social Security Numbers also make it possible for thieves to file fraudulent tax returns, file for

[28] *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 (last visited April 15, 2024).
[29] *Identity Theft and Your Social Security Number*, Social Security Administration (2018) at 1. Available at https://www.ssa.gov/pubs/EN-05-10064.pdf (last visited April 15, 2024).

unemployment benefits, or apply for a job using a false identity.[30] Each of these fraudulent activities is difficult to detect. An individual may not know that her or her Social Security Number was used to file for unemployment benefits until law enforcement notifies the individual's employer of the suspected fraud. Fraudulent tax returns are typically discovered only when an individual's authentic tax return is rejected.

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

91. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. Even then, a new Social Security number may not be effective, as "[t]he credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[31]

92. This data, as one would expect, demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "[c]ompared to credit card information, personally identifiable information and Social Security Numbers are worth more than 10x on the black market."[32]

93. 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

[30] *Id* at 4.
[31] Brian Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR (Feb. 9, 2015), http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millions-worrying-about-identity-theft (last visited April 15, 2024).
[32] Tim Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, Network World (Feb. 6, 2015), https://www.networkworld.com/article/935334/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html (last visited April 15, 2024).

compromised in this Data Breach is impossible to "close" and difficult, if not impossible, to change, e.g, SSNs, PHI, and names.

94. Because of the value of its collected and stored data, the hospitality industry has experienced disproportionally higher numbers of data theft events than other industries. Hoteliers in particular experienced several notable data breaches in recent years.[33]

95. For this reason, Defendant knew or should have known about these dangers and strengthened its data and systems accordingly. Defendant was put on notice of the substantial and foreseeable risk of harm from a data breach, yet Red Roof failed to properly prepare for that risk.

96. Defendant 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 PII, such as encrypting the information or deleting it when it is no longer needed.

97. As explained by the Federal Bureau of Investigation, "[p]revention is the most effective defense against ransomware and it is critical to take precautions for protection."[34]

98. 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;

Thoroughly investigate and remediate alerts

- Prioritize and treat commodity malware infections as potential full compromise;

[33] https://www.hoteldive.com/news/hotels-cyberattack-security/694590/ (last visited April 23, 2024).

[34] 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 (last visited April 15, 2024).

Include IT Pros in security discussions

- Ensure collaboration among [security operations], [security admins], and [information technology] admins to configure servers and other endpoints securely;

Build credential hygiene

- Use [multifactor authentication] or [network level authentication] and use strong, randomized, just-in-time local admin passwords;

Apply principle of least-privilege

- Monitor for adversarial activities
- Hunt for brute force attempts
- Monitor for cleanup of Event Logs
- Analyze logon events;

Harden infrastructure

- Use Windows Defender Firewall
- Enable tamper protection
- Enable cloud-delivered protection
- Turn on attack surface reduction rules and [Antimalware Scan Interface] for Office [Visual Basic for Applications].[35]

99. Given that Defendant was storing the Private Information of its current and former employees, Defendant could and should have implemented all of the above measures to prevent and detect cyberattacks.

100. The occurrence of the Data Breach indicates that Defendant failed to adequately implement one or more of the above measures to prevent cyberattacks, resulting in the Data Breach and the exposure of the PII of more than 27,000 current and former employees, including Plaintiffs and Class Members.

PLAINTIFFS' AND CLASS MEMBERS' DAMAGES

101. To date, Defendant has taken no actions to provide Plaintiffs and Class Members

[35] See Human-operated ransomware attacks: A preventable disaster (Mar 5, 2020), available at: https://www.microsoft.com/security/blog/2020/03/05/human-operated-ransomware-attacks-a-preventable-disaster/ (last visited April 15, 2024).

with relief for the damages they have suffered because of the Data Breach.

102. Defendant has merely offered Plaintiffs and Class Members minimal fraud and identity monitoring services, but this fails to compensate Plaintiffs and Class Members for their damages incurred and their time spent dealing with, and mitigating the effects of, the Data Breach or the lifetime risk of identity theft and fraud they now face.

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

104. Plaintiffs' and Class Members' names, dates of birth, Social Security numbers, driver's license numbers, driver's license states, state ID numbers, U.S. alien registration numbers, passport numbers, bank account numbers, routing numbers, financial documents with account numbers, credit/debit card numbers and expiration dates, security codes and pins, health insurance information, and medical information were all compromised in the Data Breach and are now in the hands of the cybercriminals who accessed Defendant's computer system.

105. Since being notified of the Data Breach, Plaintiffs have spent time dealing with the impact of the Data Breach, valuable time Plaintiffs otherwise would have spent on other activities, including but not limited to work and/or recreation.

106. Due to the Data Breach, Plaintiffs anticipate spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. This includes changing passwords, cancelling credit and debit cards, and monitoring their accounts for fraudulent activity.

107. Plaintiffs' and Class Members' Private Information was compromised as a direct and proximate result of the Data Breach.

108. As a direct and proximate result of Defendant's conduct, Plaintiffs and Class

Members have been placed at a present, imminent, immediate, and indefinite increased risk of harm from fraud and identity theft.

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

110. Plaintiffs and Class Members face substantial risk of out-of-pocket fraud losses such as loans opened in their names, medical services billed in their names, tax return fraud, utility bills opened in their names, credit card fraud, and similar identity theft.

111. Plaintiffs and Class Members face substantial risk of being targeted for future phishing, data intrusion, and other illegal schemes based on their Private Information as potential fraudsters could use that information to more effectively target such schemes to Plaintiffs and Class Members. Collectively, Plaintiffs have already experienced various phishing attempts by telephone and through electronic mail.

112. Plaintiffs and Class Members may also incur out-of-pocket costs for protective measures such as credit monitoring fees, credit report fees, credit freeze fees, and similar costs directly or indirectly related to the Data Breach.

113. Plaintiffs and Class Members also suffered a loss of value of their Private Information when it was acquired by cyber thieves in the Data Breach. Numerous courts have recognized the propriety of loss of value damages in related cases.

114. Plaintiffs and Class Members were also damaged via benefit-of-the-bargain damages. Plaintiffs and Class Members overpaid for a service that was intended to be accompanied by adequate data security that complied with industry standards but was not. Part of the wages that Defendant paid to Plaintiffs and Class Members was intended to be used by Defendant to fund adequate security of Red Roof's computer system and Plaintiffs' and Class Members' Private

Information. Thus, Plaintiffs and the Class Members did not get what they paid for and agreed to.

115. Plaintiffs and Class Members have spent and will continue to spend significant amounts of time monitoring their accounts and sensitive information for misuse.

116. Plaintiffs and Class Members have suffered or will suffer actual injury as a direct result of the Data Breach. Many victims suffered ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach relating to:

a. Reviewing and monitoring sensitive accounts and finding fraudulent insurance claims, loans, and/or government benefits claims;

b. Purchasing credit monitoring and identity theft prevention;

c. Placing "freezes" and "alerts" with reporting agencies;

d. Spending time on the phone with or at financial institutions, healthcare providers, and/or government agencies to dispute unauthorized and fraudulent activity in their name;

e. Contacting financial institutions and closing or modifying financial accounts; and,

f. Closely reviewing and monitoring Social Security Number, medical insurance accounts, bank accounts, and credit reports for unauthorized activity for years to come.

117. Moreover, Plaintiffs and Class Members have an interest in ensuring that their Private Information, which is believed to remain in the possession of Defendant, is protected from further breaches by the implementation of security measures and safeguards, including but not limited to, making sure that the storage of data or documents containing Private Information is not accessible online and that access to such data is password protected.

118. Further, as a result of Defendant's conduct, Plaintiffs and Class Members are forced to live with the anxiety that their Private Information—which contains the most intimate details about a person's life, including what ailments they suffer, whether physical or mental—may be disclosed to the entire world, thereby subjecting them to embarrassment and depriving them of any right to privacy whatsoever.

119. As a direct and proximate result of Defendant's actions and inactions, Plaintiffs and Class Members have suffered anxiety, emotional distress, and loss of privacy, and are at an increased risk of future harm.

Plaintiffs' Experiences

Plaintiff Vail Pinkston McCall

120. Plaintiff McCall is a former employee of Red Roof Inn. Upon information and belief, she was presented with standard forms to complete prior to her employment that requested her Private Information.

121. As part of her employment application and as a requirement and condition to serve as an employee for Defendant, Plaintiff McCall entrusted her Private Information to Red Roof with the reasonable expectation and understanding that Red Roof would take at a minimum reasonable security precautions to protect, maintain, and safeguard that information from unauthorized users or disclosure, and would timely notify her of any data security incidents related to her. Plaintiff McCall would not have provided Red Roof with her Private Information had she known that Red Roof would not take reasonable steps to safeguard her Private Information.

122. Plaintiff McCall is very careful about sharing her Private Information. Plaintiff Sena has never knowingly transmitted unencrypted sensitive Private Information over the internet or any other unsecured source. Plaintiff Sena stores any documents containing her sensitive Private

Information in a safe and secure location or destroys the documents.

123. In December 2023, months after Red Roof learned of the data breach, Plaintiff McCall received a letter from Red Roof, dated December 8, 2023, notifying her that her Private Information had been improperly accessed and/or obtained by unauthorized third parties. The notice indicated that Plaintiff McCall's Private Information, including her name and Social Security number.

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

125. Plaintiff McCall has spent multiple hours attempting to mitigate the effects of the breach and safeguard herself from its consequences. She will continue to spend valuable time she otherwise would have spent on other activities, including but not limited to work and/or recreation.

126. Plaintiff McCall was recently alerted that an unauthorized attempt to open a credit card in her name at Chase Bank. Plaintiff attributes this instance of fraud to the Red Roof Data Breach as she never attempted to open a credit card at Chase Bank.

127. Plaintiff McCall also suffered actual injury in the form of her Private Information being disseminated on the dark web, according to Experian, which, upon information and belief, was caused by the Data Breach.

128. Plaintiff McCall suffered actual injury from having her Private Information

compromised as a result of the Data Breach including, but not limited to (a) damage to and diminution in the value of her Private Information, a form of property that Red Roof obtained from Plaintiff; (b) violation of her privacy rights; (c) the likely theft of her Private Information; and (d) imminent and impending injury arising from the increased risk of identity theft and fraud.

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

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

Plaintiff Rebecca Richardson

131. Plaintiff Richardson is a former employee of Red Roof Inn whose employment ended in 2020. Upon information and belief, she was presented with standard forms to complete prior to her employment that requested her Private Information.

132. As part of her employment application and as a requirement and condition to serve as an employee for Defendant, Plaintiff Richardson entrusted her Private Information to Red Roof with the reasonable expectation and understanding that Red Roof would take at a minimum reasonable security precaution to protect, maintain, and safeguard that information from

unauthorized users or disclosure, and would timely notify her of any data security incidents related to her. Plaintiff Richardson would not have provided Red Roof with her Private Information had she known that Red Roof would not take reasonable steps to safeguard her Private Information.

133. Plaintiff Richardson is very careful about sharing her Private Information. Plaintiff Sena has never knowingly transmitted unencrypted sensitive Private Information over the internet or any other unsecured source. Plaintiff Sena stores any documents containing her sensitive Private Information in a safe and secure location or destroys the documents.

134. In December 2023, months after Red Roof learned of the data breach, Plaintiff Richardson received a letter from Red Roof, dated December 8, 2023, notifying her that her Private Information had been improperly accessed and/or obtained by unauthorized third parties. The notice indicated that Plaintiff Richardson's Private Information, including her name and Social Security number, were accessed and exfiltrated in the Data Breach.

135. Plaintiff Richardson has already suffered from identity theft and fraud. On or around November 20, 2023, a cybercriminal placed three fraudulent charges for $9.99 each with Plaintiff Richardson’s First Community Credit Union account.

136. In the aftermath of the Data Breach, Plaintiff Richardson has suffered from a spike in spam and scam emails, texts, and phone calls. Plaintiff Richardson was required to provide Defendant with her contact information when applying for her job, and upon information and belief, this information was compromised in the Data Breach.

137. As a result of the Data Breach, Plaintiff Richardson made reasonable efforts to mitigate the impact of the Data Breach after receiving the data breach notification letter, including but not limited to dealing with fraudulent transactions on her bank account, researching the Data Breach reviewing credit card and financial account statements. Plaintiff Richardson will continue

to spend valuable time she otherwise would have spent on other activities, including but not limited to work and/or recreation.

138. Plaintiff Richardson suffered actual injury from having her Private Information compromised as a result of the Data Breach including, but not limited to (a) damage to and diminution in the value of her Private Information, a form of property that Red Roof obtained from Plaintiff; (b) violation of her privacy rights; (c) the likely theft of her Private Information; and (d) imminent and impending injury arising from the increased risk of identity theft and fraud.

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

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

Plaintiff Viomar Sena

141. Plaintiff Sena is a former employee of Red Roof Inn whose employment ended in or around 2017. Upon information and belief, she was presented with standard forms to complete prior to her employment that requested her Private Information.

142. As part of her employment application and as a requirement and condition to serve

as an employee for Defendant, Plaintiff Sena entrusted her Private Information to Red Roof with the reasonable expectation and understanding that Red Roof would take at a minimum reasonable security precaution to protect, maintain, and safeguard that information from unauthorized users or disclosure, and would timely notify her of any data security incidents related to her. Plaintiff Sena would not have provided Red Roof with her Private Information had she known that Red Roof would not take reasonable steps to safeguard her Private Information.

143. Plaintiff Sena is very careful about sharing her Private Information. Plaintiff Sena has never knowingly transmitted unencrypted sensitive Private Information over the internet or any other unsecured source. Plaintiff Sena stores any documents containing her sensitive Private Information in a safe and secure location or destroys the documents.

144. In December 2023, months after Red Roof learned of the data breach, Plaintiff Sena received a letter from Red Roof, dated December 8, 2023, notifying her that her Private Information had been improperly accessed and/or obtained by unauthorized third parties. The notice indicated that Plaintiff Sena Private Information, including her name and Social Security number, were accessed and exfiltrated in the Data Breach.

145. As a result of the Data Breach, Plaintiff Sena made reasonable efforts to mitigate the impact of the Data Breach after receiving the data breach notification letter, including but not limited researching the Data Breach reviewing credit card and financial account statements. Plaintiff Sena will continue to spend valuable time she otherwise would have spent on other activities, including but not limited to work and/or recreation.

146. Plaintiff Sena has recently become the victim of targeted, malicious, and harassing phishing communications, including phone calls and text messages, that have caused her to lose valuable time sorting through and determining which communications, if any, she should respond

to. These targeted phishing attempts have also caused Plaintiff to temporarily lose control over her personal device.

147. Plaintiff Sena also suffered actual injury from having her Private Information compromised as a result of the Data Breach including, but not limited to (a) damage to and diminution in the value of her Private Information, a form of property that Red Roof obtained from Plaintiff; (b) violation of her privacy rights; (c) the likely theft of her Private Information; and (d) imminent and impending injury arising from the increased risk of identity theft and fraud.

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

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

CLASS ACTION ALLEGATIONS

150. Plaintiffs bring this action on behalf of themselves, and all other persons similarly situated ("the Class").

151. Plaintiffs propose the following Class definitions, subject to amendment as appropriate:

All persons Red Roof identified as being among those individuals impacted by the Data Breach, including all who were sent a notice of the Data Breach (the "Class").

152. Excluded from the Classes are Defendant's officers, directors, and employees; 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.

153. Plaintiffs reserve the right to amend or modify the Class or Subclass definitions as this case progresses.

154. Numerosity. The Members of the Class are so numerous that joinder of all of them is impracticable. While the exact number of Class Members is unknown to Plaintiffs at this time, based on information and belief, the Class consists of at least 27,327 individuals whose sensitive data was compromised in Data Breach at Red Roof.

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

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

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

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

d. Whether Defendant's data security systems prior to and during the Data Breach

were consistent with industry standards;

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

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

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

h. Whether Defendant should have discovered the Data Breach sooner;

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 breach implied contracts with Plaintiffs and Class Members;

l. Whether Defendant was unjustly enriched by unlawfully retaining a benefit conferred upon them 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, treble damages, and/or injunctive relief.

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

157. Adequacy of Representation. Plaintiffs will fairly and adequately represent and protect the interests of the Members of the Class. Plaintiffs' Counsel are competent and experienced

in litigating class actions.

158. Predominance. Defendant has engaged in a common course of conduct toward Plaintiffs and Class Members, in that all the Plaintiffs' and Class Members' data was stored on the same computer system 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.

159. 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.

160. 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.

161. Likewise, particular issues under Rule 42(d)(l) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but

are not limited to:

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

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

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

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

e. Whether Defendant failed to take commercially reasonable steps to safeguard employee Private Information; and

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

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

COUNT I
Negligence
(On Behalf of Plaintiffs and the Class)

163. Plaintiffs re-allege and incorporate by reference all other paragraphs in the Complaint as if fully set forth herein, with the exception that this claim is brought in the alternative to breach of implied contract and unjust enrichment.

164. Defendant required individuals, including Plaintiffs and Class Members, to submit non-public Private Information as a condition of employment.

165. By collecting and storing this data in its computer system and network, and sharing it and using it for commercial gain, Defendant owed a duty of care to use reasonable means to secure and safeguard its computer system—and Class Members' Private Information held within it—to prevent disclosure of the information, and to safeguard the information from theft. 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.

166. Defendant owed a duty of care to Plaintiffs and Class Members to provide reasonable data security consistent with industry standards and other requirements discussed herein, and to ensure that its systems and networks, and the personnel responsible for them, adequately protected the Private Information.

167. Defendant's duty to Plaintiffs arises independent from, and is not tethered to, any contract.

168. A special relationship that existed between Defendant and its employees, which is recognized by statutes and regulations, as well as common law. Defendant was in a superior position to ensure that its systems were sufficient to protect against the foreseeable risk of harm to Class Members from a data breach.

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

170. 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.

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

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

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

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

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

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

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

g. Maintaining Private Information for longer than it had a legitimate need; and

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

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

173. 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.

174. Plaintiffs and Class Members are entitled to compensatory and consequential

damages suffered as a result of the Data Breach.

175. Plaintiffs and Class Members are also entitled to injunctive relief requiring Defendant to, *e.g.,* (i) strengthen their 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.

176. Pursuant to the Federal Trade Commission Act, 15 U.S.C. § 45, Defendant had a duty to provide fair and adequate computer systems and data security practices to safeguard Plaintiffs and Class Members' Private Information.

177. Defendant breached its duties to Plaintiffs and Class Members under the Federal Trade Commission Act by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiffs' and Class Members' Private Information.

178. Defendant's failure to comply with applicable laws and regulations constitutes negligence per se.

179. But for Defendant's wrongful and negligent breach of their duties owed to Plaintiffs and Class Members, Plaintiffs and Class Members would not have been injured.

180. The injury and harm suffered by Plaintiffs and Class Members was the reasonably foreseeable result of Defendant's breach of their duties. Defendant knew or should have known that it was failing to meet its duties, and that Defendant's breach would cause Plaintiffs and Class Members to experience the foreseeable harms associated with the exposure of their Private Information.

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

COUNT II
Negligence *Per Se*
(On Behalf of Plaintiffs and the Class)

182. Plaintiffs re-allege and incorporate by reference all other paragraphs in the Complaint as if fully set forth herein, with the exception that this claim is brought in the alternative to breach of implied contract and unjust enrichment.

183. Under the FTC Act, 15 U.S.C. § 45, Defendant had a duty to use fair and adequate computer systems and data security practices to safeguard Plaintiffs' and Class Members' Private Information.

184. Section 5 of the FTC Act 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 the Private Information entrusted to it. The FTC publications and orders promulgated pursuant to the FTC Act also form part of the basis of Defendant's duty to protect Plaintiffs' and Class Members' Private Information.

185. Defendant breached its respective duties to Plaintiffs and Class Members under the FTC Act by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Private Information.

186. Defendant violated its duty under Section 5 of the FTC At 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 Defendant had collected and stored and the foreseeable consequences of a data breach.

187. The harm that has occurred is the type of harm the FTC Act is intended to guard against. Indeed, the FTC has pursued numerous enforcement actions against businesses that,

because 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.

188. But for Defendant's wrongful and negligent breach of its duties owed, Plaintiffs and Class Members would not have been injured.

189. The injury and harm suffered by Plaintiffs and Class Members was the reasonably foreseeable result of Defendant's breach of duties. Defendant knew or should have known that it was failing to meet its duties and that its breach would cause Plaintiffs and Class Members to suffer the foreseeable harms associated with the exposure of their Private Information.

190. Defendant's various violations and its failure to comply with applicable laws and regulations constitutes negligence *per se*.

191. As a direct and proximate result of Defendant's negligence *per se*, Plaintiffs and Class Members have suffered and will continue to suffer numerous injuries (as detailed *supra*).

COUNT III
Breach of Implied Contract
(On Behalf of Plaintiffs and the Class)

192. Plaintiffs incorporate by reference all other allegations in the Complaint as if fully set forth herein, with the exception that this claim is brought in the alternative to Plaintiffs' claims for negligence, negligence per se, and unjust enrichment.

193. Plaintiffs and the Class Members entered into implied contracts with Defendant under which Defendant agreed to safeguard and protect such information and to timely and accurately notify Plaintiffs and Class Members that their information had been breached and compromised.

194. Plaintiffs and the Class were required to and delivered their Private Information to Defendant as part of the employment process with Defendant. Plaintiffs' Private Information is a

valuable form of consideration.

195. Defendant Red Roof solicited, offered, and invited Class Members to provide their Private Information as part of Defendant's regular business practices. Plaintiffs and Class Members accepted Defendant's offers of or consideration for employment and provided their Private Information to Defendant.

196. Defendant accepted possession of Plaintiffs' and Class Members' Private Information for the purpose of employing Plaintiffs and Class Members or considering them for employment.

197. In accepting such information and payment for services, Plaintiffs and the other Class Members entered into an implied contract with Defendant whereby Defendant became obligated to reasonably safeguard Plaintiffs' and the other Class Members' Private Information.

198. The statements in Defendant's privacy policy evidence the implied understanding between Defendant and its prospective, current, and former employees.

199. In delivering their Private Information to Defendant, Plaintiffs and Class Members intended and understood that Defendant would adequately safeguard the data. Plaintiffs Private Information is itself a form of valuable consideration for this implied bargain.

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

201. The implied promises include but are not limited to: (1) taking steps to ensure that any agents who are granted access to Private Information also protect the confidentiality of that data; (2) taking steps to ensure that the information that is placed in the control of its agents is

restricted and limited to achieve an authorized medical purpose; (3) restricting access to qualified and trained agents; (4) designing and implementing appropriate retention policies to protect the information against criminal data breaches; (5) applying or requiring proper encryption; (6) multifactor authentication for access; and (7) other steps to protect against foreseeable data breaches.

202. Plaintiffs and the Class Members would not have entrusted their Private Information to Defendant in the absence of such an implied contract.

203. Had Defendant disclosed to Plaintiffs and the Class that it did not have adequate computer systems and security practices to secure sensitive data, Plaintiffs and the other Class Members would not have provided their Sensitive Information to Defendant.

204. Defendant recognized that Plaintiffs' and Class Members' Private Information is highly sensitive and must be protected, and that this protection was of material importance as part of the bargain to Plaintiffs and the other Class Members.

205. Plaintiffs and the other Class Members fully fulfilled their obligations under the implied contracts with Defendant.

206. Defendant breached the implied contract with Plaintiffs and the other Class Members by failing to take reasonable measures to safeguard their Private Information as described herein.

207. As a direct and proximate result of Defendant's conduct, Plaintiffs and the other Class Members suffered and will continue to suffer damages in an amount to be proven at trial.

COUNT IV
Invasion of Privacy
(On Behalf of Plaintiffs and the Class)

208. Plaintiffs restate and reallege allegations from the Complaint as if fully set forth

herein.

209. Plaintiffs and the Class had a legitimate expectation of privacy regarding their highly sensitive and confidential PII and were accordingly entitled to the protection of this information against disclosure to unauthorized third parties.

210. Defendant owed a duty to its employees, including Plaintiffs and the Class, to keep this information confidential.

211. Defendant intruded on Plaintiffs' and Class Members' seclusion by intentionally placing and maintaining Plaintiffs' and Class Members' PII on an unsecured network in an unencrypted manner, which Defendant knew would leave this information vulnerable to foreseeable cyberattacks. Defendant then intruded on Plaintiffs' and Class Members' seclusion and publicly disclosed their Private Information by affirmatively and intentionally, albeit under false pretenses, providing malicious cybercriminals with access to its network through what was more than likely the result of phishing or other social engineering techniques.

212. Defendant's conduct is highly offensive, outrageous, and likely to cause mental anguish to a reasonable person.

213. The intrusion was into a place or thing which was private and entitled to be private. Moreover, the disclosure was to the public at large, as evidenced by the fact that plaintiffs' Private Information has been located on the dark web.

214. Plaintiffs and the Class disclosed their sensitive and confidential information to Defendant, but did so privately, with the intention that their information would be kept confidential and protected from unauthorized disclosure. Plaintiffs and the Class were reasonable in their belief that such information would be kept private and would not be disclosed without their authorization.

215. The Data Breach constitutes an interference with Plaintiffs' and the Class's interest

in solitude or seclusion, either as to their person or as to their private affairs or concerns, of a kind that would be highly offensive to a reasonable person.

216. As a proximate result of Defendant's conduct, the private and sensitive PII of Plaintiffs and the Class was provided to a third party and is now available for disclosure and redisclosure without authorization, causing Plaintiffs and the Class to suffer injury as described throughout this Complaint.

COUNT V
Unjust Enrichment
(On Behalf of Plaintiffs and the Class)

217. Plaintiffs repeat and reallege every allegation contained in the Complaint as if fully set forth herein, with the exception that this claim is brought in the alternative to claims for negligence, negligence per se, and breach of implied contract.

218. Upon information and belief, Defendant funds its data security measures entirely from its general revenue, including funds made as a result of the labor from Plaintiffs and the Class Members.

219. As such, a portion of the revenue made as a result of the labor of Plaintiffs and the 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.

220. Plaintiffs' Private Information is itself valuable intangible property, and its conferral on Defendant was a benefit.

221. Plaintiffs and Class Members conferred a monetary benefit on Defendant. In exchange, Plaintiffs and Class Members should have received adequate data security protecting their Private Information.

222. Defendant knew that Plaintiffs and Class Members conferred a benefit which

Defendant accepted. Defendant profited from these transactions and used the Private Information of Plaintiffs and Class Members for business purposes.

223. Plaintiffs and Class Members conferred a benefit on Defendant, a portion of which was to have been used for data security measures to secure Plaintiffs' and Class Members' Personal Information, and by providing Defendant with their valuable Personal Information.

224. Defendant enriched itself by saving the costs it reasonably should have expended on data security measures to secure Plaintiffs' and Class Members' Personal Information. Instead of providing a reasonable level of security that would have prevented the Data Breach, Defendant instead calculated to avoid their data security obligations at the expense of Plaintiffs and Class Members by utilizing cheaper, ineffective security measures. Plaintiffs and Class Members, on the other hand, suffered as a direct and proximate result of Defendant's failure to provide the requisite security.

225. Under the principles of equity and good conscience, Defendant should not be permitted to retain the money that should have been used on data security, because Defendant failed to implement appropriate data management and security measures that are mandated by industry standards.

226. Defendant acquired the monetary benefit and Personal Information through inequitable means in that it failed to disclose the inadequate security practices previously alleged.

227. If Plaintiffs and Class Members knew that Defendant had not secured their Personal Information, they would not have agreed to provide their Personal Information to Defendant.

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

229. 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) actual identity theft;

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

230. 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.

231. Defendant should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiffs and Class Members, proceeds that they unjustly received from them.

COUNT VI
Declaratory Judgment
(On Behalf of Plaintiffs and the Class)

232. Plaintiffs repeat and reallege every allegation contained in the Complaint as if fully set forth herein.

233. 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. The Court has broad authority to restrain acts, such as those alleged herein, which are tortious and unlawful.

234. Defendant owes a duty of care to Plaintiffs and Class Members, requiring it to adequately secure Plaintiffs' and Class Members' Private Information.

235. Defendant still possesses Private Information regarding Plaintiffs and Class Members.

236. Plaintiffs allege that Defendant's data security measures remain inadequate. Furthermore, Plaintiffs continue to suffer injuries as a result of the compromise of their Private Information and the risks remains that further compromises of their Private Information will occur in the future.

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

a. Red Roof owes a legal duty to secure its current and former employees' Private Information from unauthorized disclosure and theft;

b. Red Roof's existing security measures do not comply with its implicit contractual obligations, and duties of care to provide reasonable security procedures and practices that are appropriate to protect current and former employees' Private Information; and

c. Red Roof continues to breach this duty by failing to employ reasonable measures to secure current and former employees' Private Information.

238. This Court should also issue corresponding prospective injunctive relief requiring Defendant to employ adequate security protocols consistent with legal and industry standards to protect current and former employees' Private Information, including the following:

a. Order Red Roof to provide lifetime credit monitoring and identity theft insurance to Plaintiffs and Class Members; and

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

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

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

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

iv. segmenting its user applications by, among other things, creating firewalls and access controls so that if one area is compromised, hackers cannot gain access to other portions of Red Roof's systems;

v. conducting regular database scanning and security checks;

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

to a breach;

vii. routinely and continually purging all former employee data that is no longer necessary in order to adequately conduct its business operations; and

viii. meaningfully educating its current and former employees about the threats they face with regard to the security of their Private Information, as well as the steps Red Roof's current and former employees should take to protect themselves.

239. If an injunction is not issued, Plaintiffs will suffer irreparable injury and will lack an adequate legal remedy to prevent another data breach at Red Roof. The risk of another such breach is real, immediate, and substantial. If another breach at Red Roof occurs, Plaintiffs will not have an adequate remedy at law because many of the resulting injuries are not readily quantifiable.

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

241. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing a subsequent data breach at Red Roof, thus preventing future injury to Plaintiffs and other current and former employees whose Private Information would be further compromised.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs pray for judgment as follows:

a. For an Order certifying this action as a Class action and appointing Plaintiffs as Class Representatives and their counsel as Class Counsel;

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

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

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

e. Ordering Defendant to pay for not less than three years of three-bureau credit monitoring services for Plaintiffs and the Class;

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

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

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

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

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

JURY TRIAL DEMANDED

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

Dated: April 29, 2024

Respectfully Submitted,

/s/ Terence R. Coates

Terence R. Coates – Trial Attorney
Jonathan T. Deters
Dylan J. Gould
MARKOVITS, STOCK & DEMARCO, LLC
119 East Court Street, Suite 530
Cincinnati, OH 45202
Phone: (513) 651-3700
Fax: (513) 665-0219
tcoates@msdlegal.com
jdeters@msdlegal.com
dgould@msdlegal.com

Gary M. Klinger (*pro hac vice*)
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN, PLLC
227 Monroe Street, Suite 2100
Chicago, IL 60606
Phone: 866.252.0878
Email: gklinger@milberg.com

Samuel J. Strauss *
Raina Borrelli (*pro hac vice*)
Brittany Resch *
TURKE & STRAUSS LLP
613 Williamson Street, Suite 201
Madison, Wisconsin 53703
Telephone: (608) 237-1775
Facsimile: (608) 509-4423
sam@turkestrauss.com
raina@turkestrauss.com
brittanyr@turkestrauss.com

Christopher D. Wiest
Chris Wiest, Attorney at Law, PLLC
50 E. Rivercenter Blvd, Ste. 1280
Covington, KY 41011

Tel: (513) 257-1895
E: chris@cwiestlaw.com

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

Plaintiffs' and Class Counsel

** Pro Have Vice Forthcoming*

CERTIFICATE OF SERVICE

The undersigned hereby certifies that on April 29, 2024, the foregoing was filed electronically. Notice of this filing will be sent to all parties by operation of the Court's electronic filing system. Parties may access this filing through the Court's system.

/s/ *Terence R. Coates*
Terence R. Coates (0085579)